SECURITY CHECKER

Powered by BLACKDUCK | HUB

YOUR CODE IS AT RISK.

Uh oh. Looks like you may have known
open source vulnerabilities
in your code.

112	37	501
Open Source Components	Vulnerable Components	Total Vulnerabilities

WHAT NOW?

Find Them: You can't manage risks if you don't know your code.
Review these open source components and vulnerabilities.

Fix Them: Use the component and vulnerability information to help you update components with known vulnerabilities.

Manage Them: Want to stay safe by automating open source vulnerability detection in your development environment? We can help!

37/112 Vulnerable Components
These open source components have known vulnerabilities.
They may need to be updated to a more current version.

Component	Version	Vulnerabilities
Apache HTTP Server	2.4.10	26
base-files	8+deb8u4	1
bash-builtins	4.3	1
Berkeley DB for .NET	5.3.28	30

DASH	0.5.7	1
Debian linux-2.6	3.16.7-ckt20	139
dpkg	1.17.26	1
file	5.22+15	3
glib2.0	2.42.1	1
GNU Binutils	2.25	1
GNU C Library	2.19	27
GNU Compiler Collection	4.9.2	1
GNU Core Utilities	8.23	4
GNU tar	1.27.1	1
GnuPG	1.4.18	1
gzip	1.6	2
inetutils-inetd	1.9.2.39.3a460	1
krb5-kdc	1.12.1+dfsg	13
libc6-dev	2.19	20
libcurl3-gnutls	7.38.0	16
libgnutls11	3.3.8	9

libjpeg	1.3.1	1
libpng	1.2.50	16
libstdc++6	4.9.2	1
libxml2	2.9.1+dfsg1	28
mount	2.25.2	2
OpenLDAP	2.4.40+dfsg	3
OpenSSL	1.0.1e	88
pam	1.1.8	5
PCRE	10.21	3
Perl	5.20.2	7
perl-base	5.20.2	7
php5-dev	5.6.21+dfsg	31
shadow	4.2	4
systemd	215	2
The GNU Ada compiler	1.4.17	2
udev	215	2

75/112 Clean Components

These open source components have no known vulnerabilities.
It's still important to continuously monitor them, as many vulnerabilities are reported months or even years after the component version is released.

Component	Version
acl	2.2.52
adduser	3.113+nmu3
apr-util	1.5.4
apt - Advanced Package Tool	1.0.9.7
Audit	2.4
base-passwd	3.5.37
bsdutils	2.25.2
ca-certificates	20141019+deb8u1
Cygwin	1.7.32
Cyrus SASL	2.1.26.dfsg1
debconf	1.5.56
debian-archive-keyring	2014.3

debian-docker-image	master-20140612
devmapper	1.02.90
Diff	3.3
Duplicate Project 283	5.6.21
e2fsprogs	1.42.12
Ecere SDK	0.44.a
epocemx	2.20
Eve ore value spreadsheet - Codeplex	eovs.v1.1
findutils	4.4.2
gettext	1.05
GNU Autoconf	2.69
GNU Ncurses	5.9+20140913
Gwyddion	2.43
HipHop Virtual Machine for PHP	HHVM-3.3.1
hippyvm	master-20140329
insserv	1.14.0

iproute	3.16.0
libbz2-1.0	1.0.6
libedit2	3.1-20140620
libgcrypt	1.6.3
libgpg-error0	1.17
libjs	1.0.0
liblua5.1-0	5.1.5
libmpfr4	3.1.2
libnettle	2.7.1
libpcap	2.24
libsemanage1	2.3
libsigsegv-dev	2.10
libssh2	1.4.3
Libtasn1	4.2
libtext-charwidth-perl	0.04
libtext-wrapi18n-perl	0.06
libusb	0.1.12

libustr-1.0-1	1.0.4
Linux Unified Key Setup	1.6.6
lsb	4.1+Debian13+nmu1
make	4.0
mawk	1.3.3
mini2440	090306
musl	1.1.9
ncurses-base	5.9+20140913
ncurses-bin	5.9+20140913
nntpgrab	0.7.2
oniguruma	0.10.0
php-net-url	1.0.15
php-src	5.6.21
php5-common	1.10.1+submodules+notgz
phpdbg	v0.3.0
pkg-config	0.28
PlexAP - beach	0.0.1

procps	3.3.9
PyqPlayer - Sharp Zaurus SDK for DSL	0.1
qtmoko	gta02-v58
re2c	0.13.5
remctl	3.9
S-Lang	2.3.0
SQLite	3.8.7.1
sysvinit	2.88dsf
Text::Iconv	1.7
tzdata	2016d
wordpress	4.5.1
wxPHP	3.0.0.2
XZ Utils	5.1.1alpha+20120614

501 Known Vulnerabilities

The following vulnerabilities are present in your code.

Click the CVE number to access the National Vulnerability Database (NVD) report. Detailed vulnerability diagnostics, including the code locations and remediation guidance is available in Black Duck Hub.

Apache HTTP Server	**2.4.10**
CVE-2010-0425	
HIGH SEVERITY	modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."
CVE-2007-6423	
HIGH SEVERITY	** DISPUTED ** Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.
CVE-2007-0086	
HIGH SEVERITY	** DISPUTED ** The Apache HTTP Server, when accessed through a TCP connection with a large window size, allows remote attackers to cause a denial of service (network bandwidth consumption) via a Range header

	that specifies multiple copies of the same fragment. NOTE: the severity of this issue has been disputed by third parties, who state that the large window size required by the attack is not normally supported or configured by the server, or that a DDoS-style attack would accomplish the same goal.
CVE-2012-0883	
MEDIUM SEVERITY	envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
CVE-2014-3523	
MEDIUM SEVERITY	Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.
CVE-2014-3583	
MEDIUM SEVERITY	The handle_headers function in mod_proxy_fcgi.c in the mod_proxy_fcgi module in the Apache HTTP Server 2.4.10

	allows remote FastCGI servers to cause a denial of service (buffer over-read and daemon crash) via long response headers.
CVE-2014-3581	
MEDIUM SEVERITY	The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.
CVE-2015-0228	
MEDIUM SEVERITY	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.
CVE-2015-3675	
MEDIUM SEVERITY	The default configuration of the Apache HTTP Server on Apple OS X before 10.10.4 does not enable the mod_hfs_apple module, which allows remote attackers to bypass HTTP authentication via a crafted URL.

CVE-2007-1862

MEDIUM SEVERITY

The recall_headers function in mod_mem_cache in Apache 2.2.4 does not properly copy all levels of header data, which can cause Apache to return HTTP headers containing previously used data, which could be used by remote attackers to obtain potentially sensitive information.

CVE-2015-3183

MEDIUM SEVERITY

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2003-1138

MEDIUM SEVERITY

The default configuration of Apache 2.0.40, as shipped with Red Hat Linux 9.0, allows remote attackers to list directory contents, even if auto indexing is turned off and there is a default web page configured, via a GET request containing a double slash (//).

CVE-2010-2068

MEDIUM SEVERITY	mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.

CVE-2015-0253

MEDIUM SEVERITY	The read_request_line function in server/protocol.c in the Apache HTTP Server 2.4.12 does not initialize the protocol structure member, which allows remote attackers to cause a denial of service (NULL pointer dereference and process crash) by sending a request that lacks a method to an installation that enables the INCLUDES filter and has an ErrorDocument 400 directive specifying a local URI.

CVE-2007-3303

MEDIUM SEVERITY	Apache httpd 2.0.59 and 2.2.4, with the Prefork MPM module, allows local users to cause a denial of service via certain code sequences executed in a worker process that (1) stop request processing by killing all

	worker processes and preventing creation of replacements or (2) hang the system by forcing the master process to fork an arbitrarily large number of worker processes. NOTE: This might be an inherent design limitation of Apache with respect to worker processes in hosted environments.
CVE-2007-1743	
MEDIUM SEVERITY	suexec in Apache HTTP Server (httpd) 2.2.3 does not verify combinations of user and group IDs on the command line, which might allow local users to leverage other vulnerabilities to create arbitrary UID/GID owned files if /proc is mounted. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root." In addition, because this is dependent on other vulnerabilities, perhaps this is resultant and should not be included in CVE.
CVE-2003-1307	
MEDIUM SEVERITY	** DISPUTED ** The mod_php module for the Apache HTTP Server allows local users with write access to PHP scripts to send signals to the server's process group and use the

	server's file descriptors, as demonstrated by sending a STOP signal, then intercepting incoming connections on the server's TCP port. NOTE: the PHP developer has disputed this vulnerability, saying "The opened file descriptors are opened by Apache. It is the job of Apache to protect them ... Not a bug in PHP."
CVE-2003-1580	
MEDIUM SEVERITY	The Apache HTTP Server 2.0.44, when DNS resolution is enabled for client IP addresses, uses a logging format that does not identify whether a dotted quad represents an unresolved IP address, which allows remote attackers to spoof IP addresses via crafted DNS responses containing numerical top-level domains, as demonstrated by a forged 123.123.123.123 domain name, related to an "Inverse Lookup Log Corruption (ILLC)" issue.
CVE-2006-4110	
MEDIUM SEVERITY	Apache 2.2.2, when running on Windows, allows remote attackers to read source code of CGI programs via a request that contains uppercase (or alternate case) characters that bypass the case-sensitive ScriptAlias directive, but allow access to the file on case-insensitive file systems.

CVE-2008-0455

MEDIUM SEVERITY

Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

CVE-2015-3185

MEDIUM SEVERITY

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2012-3502

MEDIUM SEVERITY

The proxy functionality in (1) mod_proxy_ajp.c in the mod_proxy_ajp module and (2)

	mod_proxy_http.c in the mod_proxy_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not properly determine the situations that require closing a back-end connection, which allows remote attackers to obtain sensitive information in opportunistic circumstances by reading a response that was intended for a different client.
CVE-2014-8109	
MEDIUM SEVERITY	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.
CVE-2003-1581	
LOW SEVERITY	The Apache HTTP Server 2.0.44, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text

	into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an "Inverse Lookup Log Corruption (ILLC)" issue.
CVE-2008-0456	
LOW SEVERITY	CRLF injection vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.
CVE-2001-1534	
LOW SEVERITY	mod_usertrack in Apache 1.3.11 through 1.3.20 generates session ID's using predictable information including host IP address, system time and server process ID, which allows local users to obtain session ID's and bypass authentication when these

	session ID's are used for authentication.

base-files	**8+deb8u4**
CVE-2010-0834	
HIGH SEVERITY	The base-files package before 5.0.0ubuntu7.1 on Ubuntu 9.10 and before 5.0.0ubuntu20.10.04.2 on Ubuntu 10.04 LTS, as shipped on Dell Latitude 2110 netbooks, does not require authentication for package installation, which allows remote archive servers and man-in-the-middle attackers to execute arbitrary code via a crafted package.

bash-builtins	**4.3**
CVE-2010-0002	
LOW SEVERITY	The /etc/profile.d/60alias.sh script in the Mandriva bash package for Bash 2.05b, 3.0, 3.2, 3.2.48, and 4.0 enables the --show-control-chars option in LS_OPTIONS, which allows local users to send escape sequences to terminal emulators, or hide the existence of a file, via a crafted filename.

Berkeley DB for	**5.3.28**

.NET

CVE-2015-4785

MEDIUM SEVERITY

Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2015-4764

MEDIUM SEVERITY

Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640,

	CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4786	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-2583	

MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2015-4787

MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776,

	CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4789	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, and CVE-2015-4790.
CVE-2016-0692	
MEDIUM SEVERITY	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB

	11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0689, CVE-2016-0694, and CVE-2016-3418.
CVE-2016-0694	
MEDIUM SEVERITY	Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0689, CVE-2016-0692, and CVE-2016-3418.
CVE-2015-2626	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754,

	CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2015-2624

MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2015-4780

MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2015-4781

MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776,

	CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4782	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4783	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB

	11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-2640	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782,

	CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4784	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4775	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect

	confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4754	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786,

	CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4776	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4777	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability

	than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-4778	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.

CVE-2016-0682

MEDIUM SEVERITY

Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0689, CVE-2016-0692, CVE-2016-0694, and CVE-2016-3418.

CVE-2016-3418

MEDIUM SEVERITY

Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0689, CVE-2016-0692, and CVE-2016-0694.

CVE-2016-0689

MEDIUM SEVERITY

Unspecified vulnerability in the DataStore component in Oracle Berkeley DB 11.2.5.0.32, 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, 12.1.6.0.35, and 12.1.6.1.26 allows local users to affect confidentiality, integrity, and availability via unknown

	vectors, a different vulnerability than CVE-2016-0682, CVE-2016-0692, CVE-2016-0694, and CVE-2016-3418.
CVE-2015-4790	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, and CVE-2015-4789.
CVE-2015-2656	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via

	unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and CVE-2015-4790.
CVE-2015-2654	
MEDIUM SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2583, CVE-2015-2624, CVE-2015-2626, CVE-2015-2640, CVE-2015-2656, CVE-2015-4754, CVE-2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4789, and

	CVE-2015-4790.
CVE-2015-4788	
LOW SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect integrity and availability via unknown vectors, a different vulnerability than CVE-2015-4774 and CVE-2015-4779.
CVE-2015-4774	
LOW SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect integrity and availability via unknown vectors, a different vulnerability than CVE-2015-4779 and CVE-2015-4788.
CVE-2015-4779	
LOW SEVERITY	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect integrity and availability via unknown vectors, a different vulnerability than CVE-2015-4774 and CVE-2015-4788.

DASH	**0.5.7**
CVE-2009-0854	
MEDIUM SEVERITY	Untrusted search path vulnerability in dash 0.5.4, when used as a login shell, allows local users to execute arbitrary code via a Trojan horse .profile file in the current working directory.

Debian linux-2.6	**3.16.7-ckt20**
CVE-2015-8787	
HIGH SEVERITY	The nf_nat_redirect_ipv4 function in net/netfilter/nf_nat_redirect.c in the Linux kernel before 4.4 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by sending certain IPv4 packets to an incompletely configured interface, a related issue to CVE-2003-1604.
CVE-2015-8812	
HIGH SEVERITY	drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux kernel before 4.5 does not properly identify error conditions, which allows remote attackers to execute arbitrary code or cause a denial of service

	(use-after-free) via crafted packets.
CVE-2013-4737	
HIGH SEVERITY	The CONFIG_STRICT_MEMORY_RWX implementation for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly consider certain memory sections, which makes it easier for attackers to bypass intended access restrictions by leveraging the presence of RWX memory at a fixed location.
CVE-2015-4001	
HIGH SEVERITY	Integer signedness error in the oz_hcd_get_desc_cnf function in drivers/staging /ozwpan/ozhcd.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted packet.
CVE-2015-4002	
HIGH SEVERITY	drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 does not ensure that certain length values are sufficiently large, which allows remote attackers to cause a denial of service (system crash or large loop) or possibly execute arbitrary code via a

	crafted packet, related to the (1) oz_usb_rx and (2) oz_usb_handle_ep_data functions.
CVE-2015-4004	
HIGH SEVERITY	The OZWPAN driver in the Linux kernel through 4.0.5 relies on an untrusted length field during packet parsing, which allows remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read and system crash) via a crafted packet.
CVE-2003-1604	
HIGH SEVERITY	The redirect_target function in net/ipv4/netfilter /ipt_REDIRECT.c in the Linux kernel before 2.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by sending packets to an interface that has a 0.0.0.0 IP address, a related issue to CVE-2015-8787.
CVE-2016-2070	
HIGH SEVERITY	The tcp_cwnd_reduction function in net/ipv4 /tcp_input.c in the Linux kernel before 4.3.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via crafted TCP traffic.
CVE-2015-4003	
HIGH	The oz_usb_handle_ep_data function in

SEVERITY	drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via a crafted packet.

CVE-2014-3535

HIGH SEVERITY	include/linux/netdevice.h in the Linux kernel before 2.6.36 incorrectly uses macros for netdev_printk and its related logging implementation, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) by sending invalid packets to a VxLAN interface.

CVE-2013-7445

HIGH SEVERITY	The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated by JavaScript code that creates many CANVAS elements for rendering by Chrome or Firefox.

CVE-2014-4323

HIGH SEVERITY	The mdp_lut_hw_update function in drivers/video /msm/mdp.c in the MDP display driver for the

Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain start and length values within an ioctl call, which allows attackers to gain privileges via a crafted application.

CVE-2016-1576

HIGH SEVERITY

The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program.

CVE-2016-1575

HIGH SEVERITY

The overlayfs implementation in the Linux kernel through 4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.

CVE-2016-4568

HIGH SEVERITY

drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call.

CVE-2013-1858

HIGH SEVERITY	The clone system-call implementation in the Linux kernel before 3.8.3 does not properly handle a combination of the CLONE_NEWUSER and CLONE_FS flags, which allows local users to gain privileges by calling chroot and leveraging the sharing of the / directory between a parent process and a child process.

CVE-2014-0972

HIGH SEVERITY	The kgsl graphics driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly prevent write access to IOMMU context registers, which allows local users to select a custom page table, and consequently write to arbitrary memory locations, by using a crafted GPU command stream to modify the contents of a certain register.

CVE-2016-4951

HIGH SEVERITY	The tipc_nl_publ_dump function in net/tipc /socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation.

CVE-2015-8660

HIGH SEVERITY	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.

CVE-2015-2686

HIGH SEVERITY	net/socket.c in the Linux kernel 3.19 before 3.19.3 does not validate certain range data for (1) sendto and (2) recvfrom system calls, which allows local users to gain privileges by leveraging a subsystem that uses the copy_from_iter function in the iov_iter interface, as demonstrated by the Bluetooth subsystem.

CVE-2015-8019

HIGH SEVERITY	The skb_copy_and_csum_datagram_iovec function in net/core/datagram.c in the Linux kernel 3.14.54 and 3.18.22 does not accept a length argument, which allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write system call followed by a recvmsg system call.

CVE-2015-8539

HIGH SEVERITY	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl

commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, security/keys/trusted.c, and security/keys/user_defined.c.

CVE-2015-8816

HIGH SEVERITY

The hub_activate function in drivers/usb/core/hub.c in the Linux kernel before 4.3.5 does not properly maintain a hub-interface data structure, which allows physically proximate attackers to cause a denial of service (invalid memory access and system crash) or possibly have unspecified other impact by unplugging a USB hub device.

CVE-2013-1763

HIGH SEVERITY

Array index error in the __sock_diag_rcv_msg function in net/core/sock_diag.c in the Linux kernel before 3.7.10 allows local users to gain privileges via a large family value in a Netlink message.

CVE-2016-3157

HIGH SEVERITY

The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows guest local OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by

leveraging I/O port access.

CVE-2016-0728

HIGH SEVERITY

The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.

CVE-2015-8830

HIGH SEVERITY

Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.

CVE-2012-6701

HIGH SEVERITY

Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec.

CVE-2013-4738

HIGH SEVERITY

Multiple stack-based buffer overflows in the MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android

	contributions for MSM devices and other products, allow attackers to gain privileges via (1) a crafted VIDIOC_MSM_VPE_DEQUEUE_STREAM_BUFF_INFO ioctl call, related to drivers/media/platform /msm/camera_v2/pproc/vpe/msm_vpe.c, or (2) a crafted VIDIOC_MSM_CPP_DEQUEUE_STREAM_BUFF_INFO ioctl call, related to drivers/media/platform /msm/camera_v2/pproc/cpp/msm_cpp.c.

CVE-2016-3134

HIGH SEVERITY	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.

CVE-2014-4322

HIGH SEVERITY	drivers/misc/qseecom.c in the QSEECOM driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain offset, length, and base values within an ioctl call, which allows attackers to gain privileges or cause a denial of service (memory corruption) via a crafted application.

CVE-2016-3135

HIGH SEVERITY	Integer overflow in the xt_alloc_table_info function in net/netfilter/x_tables.c in the Linux kernel through 4.5.2 on 32-bit platforms allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.

CVE-2008-4609

HIGH SEVERITY	The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.

CVE-2016-2053

HIGH SEVERITY	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c.

CVE-2016-2143

MEDIUM SEVERITY	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case

	of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include /asm/mmu_context.h and arch/s390/include /asm/pgalloc.h.
CVE-2015-8709	
MEDIUM SEVERITY	** DISPUTED ** kernel/ptrace.c in the Linux kernel through 4.4.1 mishandles uid and gid mappings, which allows local users to gain privileges by establishing a user namespace, waiting for a root process to enter that namespace with an unsafe uid or gid, and then using the ptrace system call. NOTE: the vendor states "there is no kernel bug here."
CVE-2013-1828	
MEDIUM SEVERITY	The sctp_getsockopt_assoc_stats function in net/sctp/socket.c in the Linux kernel before 3.8.4 does not validate a size value before proceeding to a copy_from_user operation, which allows local users to gain privileges via a crafted application that contains an SCTP_GET_ASSOC_STATS getsockopt system call.
CVE-2013-1943	
MEDIUM SEVERITY	The KVM subsystem in the Linux kernel before 3.0 does not check whether kernel addresses are

	specified during allocation of memory slots for use in a guest's physical address space, which allows local users to gain privileges or obtain sensitive information from kernel memory via a crafted application, related to arch/x86 /kvm/paging_tmpl.h and virt/kvm/kvm_main.c.
CVE-2015-8543	
MEDIUM SEVERITY	The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application.
CVE-2014-5332	
MEDIUM SEVERITY	Race condition in NVMap in NVIDIA Tegra Linux Kernel 3.10 alllows local users to gain privileges via a crafted NVMAP_IOC_CREATE IOCTL call, which triggers a use-after-free error, as demonstrated by using a race condition to escape the Chrome sandbox.
CVE-2013-2224	
MEDIUM SEVERITY	A certain Red Hat patch for the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 allows local users to cause a denial of service (invalid free

operation and system crash) or possibly gain privileges via a sendmsg system call with the IP_RETOPTS option, as demonstrated by hemlock.c. NOTE: this vulnerability exists because of an incorrect fix for CVE-2012-3552.

CVE-2015-3214

MEDIUM SEVERITY

The pit_ioport_read in i8254.c in the Linux kernel before 2.6.33 and QEMU before 2.3.1 does not distinguish between read lengths and write lengths, which might allow guest OS users to execute arbitrary code on the host OS by triggering use of an invalid index.

CVE-2012-4221

MEDIUM SEVERITY

Integer overflow in diagchar_core.c in the Qualcomm Innovation Center (QuIC) Diagnostics (aka DIAG) kernel-mode driver for Android 2.3 through 4.2 allows attackers to execute arbitrary code or cause a denial of service via an application that uses crafted arguments in a local diagchar_ioctl call.

CVE-2012-4220

MEDIUM SEVERITY

diagchar_core.c in the Qualcomm Innovation Center (QuIC) Diagnostics (aka DIAG) kernel-mode driver for Android 2.3 through 4.2 allows attackers to execute arbitrary code or cause a denial of service (incorrect pointer dereference) via an

application that uses crafted arguments in a local diagchar_ioctl call.

CVE-2012-4467

MEDIUM SEVERITY

The (1) do_siocgstamp and (2) do_siocgstampns functions in net/socket.c in the Linux kernel before 3.5.4 use an incorrect argument order, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (system crash) via a crafted ioctl call.

CVE-2013-4588

MEDIUM SEVERITY

Multiple stack-based buffer overflows in net/netfilter/ipvs/ip_vs_ctl.c in the Linux kernel before 2.6.33, when CONFIG_IP_VS is used, allow local users to gain privileges by leveraging the CAP_NET_ADMIN capability for (1) a getsockopt system call, related to the do_ip_vs_get_ctl function, or (2) a setsockopt system call, related to the do_ip_vs_set_ctl function.

CVE-2013-1935

MEDIUM SEVERITY

A certain Red Hat patch to the KVM subsystem in the kernel package before 2.6.32-358.11.1.el6 on Red Hat Enterprise Linux (RHEL) 6 does not properly implement the PV EOI feature, which allows guest OS users to cause a denial of service (host OS crash) by leveraging a time window

	during which interrupts are disabled but copy_to_user function calls are possible.
CVE-2015-8550	
MEDIUM SEVERITY	Xen, when used on a system providing PV backends, allows local guest OS administrators to cause a denial of service (host OS crash) or gain privileges by writing to memory shared between the frontend and backend, aka a double fetch vulnerability.
CVE-2016-0723	
MEDIUM SEVERITY	Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linux kernel through 4.4.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free and system crash) by making a TIOCGETD ioctl call during processing of a TIOCSETD ioctl call.
CVE-2013-7446	
MEDIUM SEVERITY	Use-after-free vulnerability in net/unix/af_unix.c in the Linux kernel before 4.3.3 allows local users to bypass intended AF_UNIX socket permissions or cause a denial of service (panic) via crafted epoll_ctl calls.
CVE-2015-8767	

MEDIUM SEVERITY	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.

CVE-2016-2117

MEDIUM SEVERITY	The atl2_probe function in drivers/net/ethernet /atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.

CVE-2010-4563

MEDIUM SEVERITY	The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping.

CVE-2004-0230

MEDIUM SEVERITY	TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such

as BGP.

CVE-2016-0821

MEDIUM SEVERITY

The LIST_POISON feature in include/linux /poison.h in the Linux kernel before 4.3, as used in Android 6.0.1 before 2016-03-01, does not properly consider the relationship to the mmap_min_addr value, which makes it easier for attackers to bypass a poison-pointer protection mechanism by triggering the use of an uninitialized list entry, aka Android internal bug 26186802, a different vulnerability than CVE-2015-3636.

CVE-2015-7833

MEDIUM SEVERITY

The usbvision driver in the Linux kernel package 3.10.0-123.20.1.el7 through 3.10.0-229.14.1.el7 in Red Hat Enterprise Linux (RHEL) 7.1 allows physically proximate attackers to cause a denial of service (panic) via a nonzero bInterfaceNumber value in a USB device descriptor.

CVE-2015-7799

MEDIUM SEVERITY

The slhc_init function in drivers/net/slip/slhc.c in the Linux kernel through 4.2.3 does not ensure that certain slot numbers are valid, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted PPPIOCSMAXCID ioctl call.

CVE-2005-3660

MEDIUM SEVERITY

Linux kernel 2.4 and 2.6 allows attackers to cause a denial of service (memory exhaustion and panic) by creating a large number of connected file descriptors or socketpairs and setting a large data transfer buffer, then preventing Linux from being able to finish the transfer by causing the process to become a zombie, or closing the file descriptor without closing an associated reference.

CVE-2016-2550

MEDIUM SEVERITY

The Linux kernel before 4.5 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by leveraging incorrect tracking of descriptor ownership and sending each descriptor over a UNIX socket before closing it. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-4312.

CVE-2013-3226

MEDIUM SEVERITY

The sco_sock_recvmsg function in net/bluetooth /sco.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.

CVE-2013-4312

MEDIUM SEVERITY	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix /garbage.c.

CVE-2015-1339

MEDIUM SEVERITY	Memory leak in the cuse_channel_release function in fs/fuse/cuse.c in the Linux kernel before 4.4 allows local users to cause a denial of service (memory consumption) or possibly have unspecified other impact by opening /dev/cuse many times.

CVE-2015-7550

MEDIUM SEVERITY	The keyctl_read_key function in security/keys /keyctl.c in the Linux kernel before 4.3.4 does not properly use a semaphore, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted application that leverages a race condition between keyctl_revoke and keyctl_read calls.

CVE-2015-1573

MEDIUM SEVERITY	The nft_flush_table function in net/netfilter /nf_tables_api.c in the Linux kernel before 3.18.5 mishandles the interaction between cross-chain

	jumps and ruleset flushes, which allows local users to cause a denial of service (panic) by leveraging the CAP_NET_ADMIN capability.
CVE-2016-2384	
MEDIUM SEVERITY	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.
CVE-2016-2782	
MEDIUM SEVERITY	The treo_attach function in drivers/usb/serial /visor.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a (1) bulk-in or (2) interrupt-in endpoint.
CVE-2013-3230	
MEDIUM SEVERITY	The l2tp_ip6_recvmsg function in net/l2tp /l2tp_ip6.c in the Linux kernel before 3.9-rc7 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.

CVE-2013-3237

MEDIUM SEVERITY	The vsock_stream_sendmsg function in net/vmw_vsock/af_vsock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.

CVE-2013-3236

MEDIUM SEVERITY	The vmci_transport_dgram_dequeue function in net/vmw_vsock/vmci_transport.c in the Linux kernel before 3.9-rc7 does not properly initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.

CVE-2016-2548

MEDIUM SEVERITY	sound/core/timer.c in the Linux kernel before 4.4.1 retains certain linked lists after a close or stop action, which allows local users to cause a denial of service (system crash) via a crafted ioctl call, related to the (1) snd_timer_close and (2) _snd_timer_stop functions.

CVE-2013-3233

MEDIUM SEVERITY	The llcp_sock_recvmsg function in net/nfc /llcp/sock.c in the Linux kernel before 3.9-rc7 does

	not initialize a certain length variable and a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3232	
MEDIUM SEVERITY	The nr_recvmsg function in net/netrom /af_netrom.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2016-2543	
MEDIUM SEVERITY	The snd_seq_ioctl_remove_events function in sound/core/seq/seq_clientmgr.c in the Linux kernel before 4.4.1 does not verify FIFO assignment before proceeding with FIFO clearing, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted ioctl call.
CVE-2013-0290	
MEDIUM SEVERITY	The __skb_recv_datagram function in net/core /datagram.c in the Linux kernel before 3.8 does not properly handle the MSG_PEEK flag with zero-length data, which allows local users to cause a denial of service (infinite loop and system hang) via a crafted application.

CVE-2013-6392

MEDIUM SEVERITY

The genlock_dev_ioctl function in genlock.c in the Genlock driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted GENLOCK_IOC_EXPORT ioctl call.

CVE-2015-8785

MEDIUM SEVERITY

The fuse_fill_write_pages function in fs/fuse/file.c in the Linux kernel before 4.4 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers a zero length for the first segment of an iov.

CVE-2015-2672

MEDIUM SEVERITY

The xsave/xrstor implementation in arch/x86 /include/asm/xsave.h in the Linux kernel before 3.19.2 creates certain .altinstr_replacement pointers and consequently does not provide any protection against instruction faulting, which allows local users to cause a denial of service (panic) by triggering a fault, as demonstrated by an unaligned memory operand or a non-canonical address memory operand.

CVE-2015-4177

MEDIUM SEVERITY	The collect_mounts function in fs/namespace.c in the Linux kernel before 4.0.5 does not properly consider that it may execute after a path has been unmounted, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call.

CVE-2015-4178

MEDIUM SEVERITY	The fs_pin implementation in the Linux kernel before 4.0.5 does not ensure the internal consistency of a certain list data structure, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call, related to fs/fs_pin.c and include/linux/fs_pin.h.

CVE-2015-7566

MEDIUM SEVERITY	The clie_5_attach function in drivers/usb/serial /visor.c in the Linux kernel through 4.4.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a bulk-out endpoint.

CVE-2015-7513

MEDIUM SEVERITY	arch/x86/kvm/x86.c in the Linux kernel before 4.4 does not reset the PIT counter values during state

	restoration, which allows guest OS users to cause a denial of service (divide-by-zero error and host OS crash) via a zero value, related to the kvm_vm_ioctl_set_pit and kvm_vm_ioctl_set_pit2 functions.
CVE-2015-7515	
MEDIUM SEVERITY	The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device that lacks endpoints.
CVE-2015-8845	
MEDIUM SEVERITY	The tm_reclaim_thread function in arch/powerpc/kernel/process.c in the Linux kernel before 4.4.1 on powerpc platforms does not ensure that TM suspend mode exists before proceeding with a tm_reclaim call, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.
CVE-2016-3689	
MEDIUM SEVERITY	The ims_pcu_parse_cdc_data function in drivers/input/misc/ims-pcu.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (system crash) via a USB device without both a master and a slave

interface.

CVE-2016-2186

MEDIUM SEVERITY

The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2016-2188

MEDIUM SEVERITY

The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2016-2184

MEDIUM SEVERITY

The create_fixed_stream_quirk function in sound/usb/quirks.c in the snd-usb-audio driver in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference or double free, and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2016-2185

MEDIUM SEVERITY	The ati_remote2_probe function in drivers/input /misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2016-3140

MEDIUM SEVERITY	The digi_port_init function in drivers/usb/serial /digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2014-7207

MEDIUM SEVERITY	A certain Debian patch to the IPv6 implementation in the Linux kernel 3.2.x through 3.2.63 does not properly validate arguments in ipv6_select_ident function calls, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging (1) tun or (2) macvtap device access.

CVE-2013-4739

MEDIUM SEVERITY	The MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to obtain sensitive

	information from kernel stack memory via (1) a crafted MSM_MCR_IOCTL_EVT_GET ioctl call, related to drivers/media/platform /msm/camera_v1/mercury/msm_mercury_sync.c, or (2) a crafted MSM_JPEG_IOCTL_EVT_GET ioctl call, related to drivers/media/platform /msm/camera_v2/jpeg_10/msm_jpeg_sync.c.
CVE-2013-4220	
MEDIUM SEVERITY	The bad_mode function in arch/arm64/kernel /traps.c in the Linux kernel before 3.9.5 on the ARM64 platform allows local users to cause a denial of service (system crash) via vectors involving an attempted register access that triggers an unexpected value in the Exception Syndrome Register (ESR).
CVE-2016-3136	
MEDIUM SEVERITY	The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors.
CVE-2016-3137	
MEDIUM SEVERITY	drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically proximate

attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both an interrupt-in and an interrupt-out endpoint descriptor, related to the cypress_generic_port_probe and cypress_open functions.

CVE-2016-3138

MEDIUM SEVERITY

The acm_probe function in drivers/usb/class /cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both a control and a data endpoint descriptor.

CVE-2016-3139

MEDIUM SEVERITY

The wacom_probe function in drivers/input/tablet /wacom_sys.c in the Linux kernel before 3.17 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.

CVE-2014-8480

MEDIUM SEVERITY

The instruction decoder in arch/x86 /kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 lacks intended decoder-table flags for certain RIP-relative instructions, which allows guest OS users to cause

	a denial of service (NULL pointer dereference and host OS crash) via a crafted application.
CVE-2014-8481	
MEDIUM SEVERITY	The instruction decoder in arch/x86 /kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 does not properly handle invalid instructions, which allows guest OS users to cause a denial of service (NULL pointer dereference and host OS crash) via a crafted application that triggers (1) an improperly fetched instruction or (2) an instruction that occupies too many bytes. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8480.
CVE-2016-2847	
MEDIUM SEVERITY	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes.
CVE-2013-2890	
MEDIUM SEVERITY	drivers/hid/hid-sony.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SONY is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.

CVE-2016-2546

MEDIUM SEVERITY

sound/core/timer.c in the Linux kernel before 4.4.1 uses an incorrect type of mutex, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.

CVE-2016-2547

MEDIUM SEVERITY

sound/core/timer.c in the Linux kernel before 4.4.1 employs a locking approach that does not consider slave timer instances, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.

CVE-2016-2544

MEDIUM SEVERITY

Race condition in the queue_delete function in sound/core/seq/seq_queue.c in the Linux kernel before 4.4.1 allows local users to cause a denial of service (use-after-free and system crash) by making an ioctl call at a certain time.

CVE-2016-2545

MEDIUM SEVERITY

The snd_timer_interrupt function in sound/core /timer.c in the Linux kernel before 4.4.1 does not properly maintain a certain linked list, which allows local users to cause a denial of service (race condition and system crash) via a crafted ioctl call.

CVE-2013-2239

MEDIUM SEVERITY

vzkernel before 042stab080.2 in the OpenVZ modification for the Linux kernel 2.6.32 does not initialize certain length variables, which allows local users to obtain sensitive information from kernel stack memory via (1) a crafted ploop driver ioctl call, related to the ploop_getdevice_ioc function in drivers/block/ploop/dev.c, or (2) a crafted quotactl system call, related to the compat_quotactl function in fs/quota/quota.c.

CVE-2015-8844

MEDIUM SEVERITY

The signal implementation in the Linux kernel before 4.3.5 on powerpc platforms does not check for an MSR with both the S and T bits set, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.

CVE-2013-4129

MEDIUM SEVERITY

The bridge multicast implementation in the Linux kernel through 3.10.3 does not check whether a certain timer is armed before modifying the timeout value of that timer, which allows local users to cause a denial of service (BUG and system crash) via vectors involving the shutdown of a KVM virtual machine, related to net/bridge /br_mdb.c and net/bridge/br_multicast.c.

CVE-2013-2188

MEDIUM SEVERITY

A certain Red Hat patch to the do_filp_open function in fs/namei.c in the kernel package before 2.6.32-358.11.1.el6 on Red Hat Enterprise Linux (RHEL) 6 does not properly handle failure to obtain write permissions, which allows local users to cause a denial of service (system crash) by leveraging access to a filesystem that is mounted read-only.

CVE-2015-8551

MEDIUM SEVERITY

The PCI backend driver in Xen, when running on an x86 system and using Linux 3.1.x through 4.3.x as the driver domain, allows local guest administrators to hit BUG conditions and cause a denial of service (NULL pointer dereference and host OS crash) by leveraging a system with access to a passed-through MSI or MSI-X capable physical PCI device and a crafted sequence of XEN_PCI_OP_* operations, aka "Linux pciback missing sanity checks."

CVE-2015-8104

MEDIUM SEVERITY

The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #DB (aka Debug) exceptions, related to svm.c.

CVE-2012-4542

MEDIUM SEVERITY

block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authorization of SCSI commands, which allows local users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.

CVE-2014-2739

MEDIUM SEVERITY

The cma_req_handler function in drivers/infiniband/core/cma.c in the Linux kernel 3.14.x through 3.14.1 attempts to resolve an RDMA over Converged Ethernet (aka RoCE) address that is properly resolved within a different module, which allows remote attackers to cause a denial of service (incorrect pointer dereference and system crash) via crafted network traffic.

CVE-2016-2854

MEDIUM SEVERITY

The aufs module for the Linux kernel 3.x and 4.x does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.

CVE-2016-2069

MEDIUM SEVERITY

Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain

	privileges by triggering access to a paging structure by a different CPU.
CVE-2016-2853	
MEDIUM SEVERITY	The aufs module for the Linux kernel 3.x and 4.x does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an aufs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program.
CVE-2012-4222	
MEDIUM SEVERITY	drivers/gpu/msm/kgsl.c in the Qualcomm Innovation Center (QuIC) Graphics KGSL kernel-mode driver for Android 2.3 through 4.2 allows attackers to cause a denial of service (NULL pointer dereference) via an application that uses crafted arguments in a local kgsl_ioctl call.
CVE-2014-9717	
LOW SEVERITY	fs/namespace.c in the Linux kernel before 4.0.2 processes MNT_DETACH umount2 system calls without verifying that the MNT_LOCKED flag is unset, which allows local users to bypass intended access restrictions and navigate to filesystem locations beneath a mount by calling umount2 within a user namespace.
CVE-2007-3719	

LOW SEVERITY	The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in "Secretly Monopolizing the CPU Without Superuser Privileges."

CVE-2016-2383

LOW SEVERITY	The adjust_branches function in kernel/bpf /verifier.c in the Linux kernel before 4.5 does not consider the delta in the backward-jump case, which allows local users to obtain sensitive information from kernel memory by creating a packet filter and then loading crafted BPF instructions.

CVE-2006-6128

LOW SEVERITY	The ReiserFS functionality in Linux kernel 2.6.18, and possibly other versions, allows local users to cause a denial of service via a malformed ReiserFS file system that triggers memory corruption when a sync is performed.

CVE-2016-2549

LOW SEVERITY	sound/core/hrtimer.c in the Linux kernel before 4.4.1 does not prevent recursive callback access, which allows local users to cause a denial of service (deadlock) via a crafted ioctl call.

CVE-2015-1350

LOW SEVERITY

The VFS subsystem in the Linux kernel 3.x provides an incomplete set of requirements for setattr operations that underspecifies removing extended privilege attributes, which allows local users to cause a denial of service (capability stripping) via a failed invocation of a system call, as demonstrated by using chown to remove a capability from the ping or Wireshark dumpcap program.

CVE-2016-2085

LOW SEVERITY

The evm_verify_hmac function in security/integrity/evm/evm_main.c in the Linux kernel before 4.5 does not properly copy data, which makes it easier for local users to forge MAC values via a timing side-channel attack.

CVE-2015-8374

LOW SEVERITY

fs/btrfs/inode.c in the Linux kernel before 4.3.3 mishandles compressed inline extents, which allows local users to obtain sensitive pre-truncation information from a file via a clone action.

CVE-2015-0777

LOW SEVERITY

drivers/xen/usbback/usbback.c in linux-2.6.18-xen-3.4.0 (aka the Xen 3.4.x support patches for

	the Linux kernel 2.6.18), as used in the Linux kernel 2.6.x and 3.x in SUSE Linux distributions, allows guest OS users to obtain sensitive information from uninitialized locations in host OS kernel memory via unspecified vectors.
CVE-2015-4176	
LOW SEVERITY	fs/namespace.c in the Linux kernel before 4.0.2 does not properly support mount connectivity, which allows local users to read arbitrary files by leveraging user-namespace root access for deletion of a file or directory.
CVE-2016-3961	
LOW SEVERITY	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area.
CVE-2008-7316	
LOW SEVERITY	mm/filemap.c in the Linux kernel before 2.6.25 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers an iovec of zero length, followed by a page fault for an iovec of nonzero length.
CVE-2016-3156	

LOW SEVERITY	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.

CVE-2015-8553

LOW SEVERITY	Xen allows guest OS users to obtain sensitive information from uninitialized locations in host OS kernel memory by not enabling memory and I/O decoding control bits. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-0777.

CVE-2015-8575

LOW SEVERITY	The sco_sock_bind function in net/bluetooth/sco.c in the Linux kernel before 4.3.4 does not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application.

CVE-2016-0823

LOW SEVERITY	The pagemap_open function in fs/proc /task_mmu.c in the Linux kernel before 3.19.3, as used in Android 6.0.1 before 2016-03-01, allows local users to obtain sensitive physical-address information by reading a pagemap file, aka Android internal bug 25739721.

CVE-2015-7885

LOW SEVERITY

The dgnc_mgmt_ioctl function in drivers/staging/dgnc/dgnc_mgmt.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application.

CVE-2013-2636

LOW SEVERITY

net/bridge/br_mdb.c in the Linux kernel before 3.8.4 does not initialize certain structures, which allows local users to obtain sensitive information from kernel memory via a crafted application.

CVE-2015-8569

LOW SEVERITY

The (1) pptp_bind and (2) pptp_connect functions in drivers/net/ppp/pptp.c in the Linux kernel through 4.3.3 do not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application.

CVE-2015-8839

LOW SEVERITY

Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated

	with a different user's file after unsynchronized hole punching and page-fault handling.
CVE-2012-6543	
LOW SEVERITY	The l2tp_ip6_getname function in net/l2tp /l2tp_ip6.c in the Linux kernel before 3.6 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2015-7884	
LOW SEVERITY	The vivid_fb_ioctl function in drivers/media /platform/vivid/vivid-osd.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application.
CVE-2015-8552	
LOW SEVERITY	The PCI backend driver in Xen, when running on an x86 system and using Linux 3.1.x through 4.3.x as the driver domain, allows local guest administrators to generate a continuous stream of WARN messages and cause a denial of service (disk consumption) by leveraging a system with access to a passed-through MSI or MSI-X capable physical PCI device and XEN_PCI_OP_enable_msi operations, aka "Linux pciback missing sanity checks."

dpkg	**1.17.26**
CVE-2006-0300	
MEDIUM SEVERITY	Buffer overflow in tar 1.14 through 1.15.90 allows user-assisted attackers to cause a denial of service (application crash) and possibly execute code via unspecified vectors involving PAX extended headers.

file	**5.22+15**
CVE-2015-4604	
MEDIUM SEVERITY	The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.
CVE-2015-4605	
MEDIUM SEVERITY	The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP

	before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.
CVE-2013-4636	
MEDIUM SEVERITY	The mget function in libmagic/softmagic.c in the Fileinfo component in PHP 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) via an MP3 file that triggers incorrect MIME type detection during access to an finfo object.

glib2.0	**2.42.1**
CVE-2012-0039	
MEDIUM SEVERITY	** DISPUTED ** GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that

	maintains a hash table. NOTE: this issue may be disputed by the vendor; the existence of the g_str_hash function is not a vulnerability in the library, because callers of g_hash_table_new and g_hash_table_new_full can specify an arbitrary hash function that is appropriate for the application.

GNU Binutils	**2.25**
CVE-2006-0646	
MEDIUM SEVERITY	ld in SUSE Linux 9.1 through 10.0, and SLES 9, in certain circumstances when linking binaries, can leave an empty RPATH or RUNPATH, which allows local attackers to execute arbitrary code as other users via by running an ld-linked application from the current directory, which could contain an attacker-controlled library file.

GNU C Library	**2.19**
CVE-2014-9402	
HIGH SEVERITY	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote

	attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.
CVE-2015-1472	
HIGH SEVERITY	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf call.
CVE-2014-9761	
HIGH SEVERITY	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.
CVE-2015-8778	
HIGH SEVERITY	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r

	function, which triggers out-of-bounds heap-memory access.
CVE-2015-8779	
HIGH SEVERITY	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.
CVE-2014-4043	
HIGH SEVERITY	The posix_spawn_file_actions_addopen function in glibc before 2.20 does not copy its path argument in accordance with the POSIX specification, which allows context-dependent attackers to trigger use-after-free vulnerabilities.
CVE-2016-2856	
HIGH SEVERITY	pt_chown in the glibc package before 2.19-18+deb8u4 on Debian jessie; the elibc package before 2.15-0ubuntu10.14 on Ubuntu 12.04 LTS and before 2.19-0ubuntu6.8 on Ubuntu 14.04 LTS; and the glibc package before 2.21-0ubuntu4.2 on Ubuntu 15.10 and before 2.23-0ubuntu1 on Ubuntu 16.04 LTS and 16.10 lacks a namespace check associated with file-descriptor passing, which allows local

	users to capture keystrokes and spoof data, and possibly gain privileges, via pts read and write operations, related to debian/sysdeps /linux.mk. NOTE: this is not considered a vulnerability in the upstream GNU C Library because the upstream documentation has a clear security recommendation against the --enable-pt_chown option.
CVE-2015-5277	
HIGH SEVERITY	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
CVE-2005-0403	
HIGH SEVERITY	init_dev in tty_io.c in the Red Hat backport of NPTL to Red Hat Enterprise Linux 3 does not properly clear controlling tty's in multi-threaded applications, which allows local users to cause a denial of service (crash) and possibly gain tty access via unknown attack vectors that trigger an access of a pointer to a freed structure.
CVE-2011-0536	

MEDIUM SEVERITY	Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc or libc6), including glibc-2.5-49.el5_5.6 and glibc-2.12-1.7.el6_0.3 in Red Hat Enterprise Linux, allow local users to gain privileges via a crafted dynamic shared object (DSO) in a subdirectory of the current working directory during execution of a (1) setuid or (2) setgid program that has $ORIGIN in (a) RPATH or (b) RUNPATH within the program itself or a referenced library. NOTE: this issue exists because of an incorrect fix for CVE-2010-3847.

CVE-2014-0475

MEDIUM SEVERITY	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.

CVE-2011-2702

MEDIUM SEVERITY	Integer signedness error in Glibc before 2.13 and eglibc before 2.13, when using Supplemental Streaming SIMD Extensions 3 (SSSE3) optimization, allows context-dependent attackers to execute arbitrary code via a

	negative length parameter to (1) memcpy-ssse3-rep.S, (2) memcpy-ssse3.S, or (3) memset-sse2.S in sysdeps/i386 /i686/multiarch/, which triggers an out-of-bounds read, as demonstrated using the memcpy function.
CVE-2015-7547	
MEDIUM SEVERITY	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.
CVE-2015-1781	
MEDIUM SEVERITY	Buffer overflow in the gethostbyname_r and other unspecified NSS functions in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response, which triggers a call with a misaligned buffer.
CVE-2015-1473	

MEDIUM SEVERITY	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during a risk-management decision for use of the alloca function, which might allow context-dependent attackers to cause a denial of service (segmentation violation) or overwrite memory locations beyond the stack boundary via a long line containing wide characters that are improperly handled in a wscanf call.

CVE-2015-8776

MEDIUM SEVERITY	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.

CVE-2010-4052

MEDIUM SEVERITY	Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for

	ProFTPD.
CVE-2010-4051	
MEDIUM SEVERITY	The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."
CVE-2013-7423	
MEDIUM SEVERITY	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of request that trigger a call to the getaddrinfo function.
CVE-2015-5229	
MEDIUM SEVERITY	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly initialize memory areas, which might allow context-dependent attackers to

	cause a denial of service (hang or crash) via unspecified vectors.
CVE-2016-1234	
MEDIUM SEVERITY	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.
CVE-2014-8121	
MEDIUM SEVERITY	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up on a database while iterating over it, which triggers the file pointer to be reset.
CVE-2014-6040	
MEDIUM SEVERITY	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.

CVE-2009-0537

MEDIUM SEVERITY

Integer overflow in the fts_build function in fts.c in libc in (1) OpenBSD 4.4 and earlier and (2) Microsoft Interix 6.0 build 10.0.6030.0 allows context-dependent attackers to cause a denial of service (application crash) via a deep directory tree, related to the fts_level structure member, as demonstrated by (a) du, (b) rm, (c) chmod, and (d) chgrp on OpenBSD; and (e) SearchIndexer.exe on Vista Enterprise.

CVE-2010-4756

MEDIUM SEVERITY

The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.

CVE-2013-2207

LOW SEVERITY

pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file system.

CVE-2015-8777

LOW SEVERITY	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.

GNU Compiler Collection	**4.9.2**

CVE-2015-5276

MEDIUM SEVERITY	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not properly handle short reads from blocking sources, which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.

GNU Core Utilities	**8.23**

CVE-2009-4135

MEDIUM SEVERITY	The distcheck rule in dist-check.mk in GNU coreutils 5.2.1 through 8.1 allows local users to gain privileges via a symlink attack on a file in a directory tree under /tmp.

CVE-2013-0221	
MEDIUM SEVERITY	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the sort command, when using the (1) -d or (2) -M switch, which triggers a stack-based buffer overflow in the alloca function.
CVE-2013-0222	
LOW SEVERITY	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the uniq command, which triggers a stack-based buffer overflow in the alloca function.
CVE-2013-0223	
LOW SEVERITY	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the join command, when using the -i switch, which triggers a stack-based buffer overflow in the alloca function.

GNU tar	**1.27.1**

CVE-2005-2541

HIGH SEVERITY

Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may allow local users or remote attackers to gain privileges.

GnuPG **1.4.18**

CVE-2008-1530

HIGH SEVERITY

GnuPG (gpg) 1.4.8 and 2.0.8 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted duplicate keys that are imported from key servers, which triggers "memory corruption around deduplication of user IDs."

gzip **1.6**

CVE-2004-0603

HIGH SEVERITY

gzexe in gzip 1.3.3 and earlier will execute an argument when the creation of a temp file fails instead of exiting the program, which could allow remote attackers or local users to execute arbitrary commands, a different vulnerability than CVE-1999-1332.

CVE-2004-1349

LOW SEVERITY	gzip before 1.3 in Solaris 8, when called with the -f or -force flags, will change the permissions of files that are hard linked to the target files, which allows local users to view or modify these files.

inetutils-inetd	**1.9.2.39.3a460**

CVE-2004-1485

HIGH SEVERITY	Buffer overflow in the TFTP client in InetUtils 1.4.2 allows remote malicious DNS servers to execute arbitrary code via a large DNS response that is handled by the gethostbyname function.

krb5-kdc	**1.12.1+dfsg**

CVE-2003-0041

HIGH SEVERITY	Kerberos FTP client allows remote FTP sites to execute arbitrary code via a pipe (|) character in a filename that is retrieved by the client.

CVE-2015-2698

HIGH SEVERITY	The iakerb_gss_export_sec_context function in lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka

	krb5) 1.14 pre-release 2015-09-14 improperly accesses a certain pointer, which allows remote authenticated users to cause a denial of service (memory corruption) or possibly have unspecified other impact by interacting with an application that calls the gss_export_sec_context function. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-2696.
CVE-2015-2696	
HIGH SEVERITY	lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a gss_inquire_context call.
CVE-2015-2695	
HIGH SEVERITY	lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted SPNEGO packet that is mishandled during a gss_inquire_context call.
CVE-2015-2697	

MEDIUM SEVERITY	The build_principal_va function in lib/krb5 /krb/bld_princ.c in MIT Kerberos 5 (aka krb5) before 1.14 allows remote authenticated users to cause a denial of service (out-of-bounds read and KDC crash) via an initial '\0' character in a long realm field within a TGS request.

CVE-2015-8631

MEDIUM SEVERITY	Multiple memory leaks in kadmin/server /server_stubs.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (memory consumption) via a request specifying a NULL principal name.

CVE-2015-2694

MEDIUM SEVERITY	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track whether a client's request has been validated, which allows remote attackers to bypass an intended preauthentication requirement by providing (1) zero bytes of data or (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.

CVE-2011-0283

MEDIUM	The Key Distribution Center (KDC) in MIT

SEVERITY	Kerberos 5 (aka krb5) 1.9 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a malformed request packet that does not trigger a response packet.

CVE-2006-6144

MEDIUM SEVERITY	The "mechglue" abstraction interface of the GSS-API library for Kerberos 5 1.5 through 1.5.1, as used in Kerberos administration daemon (kadmind) and other products that use this library, allows remote attackers to cause a denial of service (crash) via unspecified vectors that cause mechglue to free uninitialized pointers.

CVE-2015-8630

MEDIUM SEVERITY	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.

CVE-2016-3119

LOW	The process_db_args function in plugins/kdb

SEVERITY	/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2004-0971	
LOW SEVERITY	The krb5-send-pr script in the kerberos5 (krb5) package in Trustix Secure Linux 1.5 through 2.1, and possibly other operating systems, allows local users to overwrite files via a symlink attack on temporary files.
CVE-2015-8629	
LOW SEVERITY	The xdr_nullstring function in lib/kadm5/kadm_rpc_xdr.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 does not verify whether '\0' characters exist as expected, which allows remote authenticated users to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted string.

libc6-dev	**2.19**

CVE-2015-8778

HIGH SEVERITY

Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.

CVE-2015-8779

HIGH SEVERITY

Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.

CVE-2014-9761

HIGH SEVERITY

Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.

CVE-2016-2856

HIGH

pt_chown in the glibc package before

SEVERITY	2.19-18+deb8u4 on Debian jessie; the elibc package before 2.15-0ubuntu10.14 on Ubuntu 12.04 LTS and before 2.19-0ubuntu6.8 on Ubuntu 14.04 LTS; and the glibc package before 2.21-0ubuntu4.2 on Ubuntu 15.10 and before 2.23-0ubuntu1 on Ubuntu 16.04 LTS and 16.10 lacks a namespace check associated with file-descriptor passing, which allows local users to capture keystrokes and spoof data, and possibly gain privileges, via pts read and write operations, related to debian/sysdeps /linux.mk. NOTE: this is not considered a vulnerability in the upstream GNU C Library because the upstream documentation has a clear security recommendation against the --enable-pt_chown option.
CVE-2015-5277	
HIGH SEVERITY	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
CVE-2005-0403	
HIGH	init_dev in tty_io.c in the Red Hat backport of

SEVERITY	NPTL to Red Hat Enterprise Linux 3 does not properly clear controlling tty's in multi-threaded applications, which allows local users to cause a denial of service (crash) and possibly gain tty access via unknown attack vectors that trigger an access of a pointer to a freed structure.

CVE-2011-0536

MEDIUM SEVERITY	Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc or libc6), including glibc-2.5-49.el5_5.6 and glibc-2.12-1.7.el6_0.3 in Red Hat Enterprise Linux, allow local users to gain privileges via a crafted dynamic shared object (DSO) in a subdirectory of the current working directory during execution of a (1) setuid or (2) setgid program that has $ORIGIN in (a) RPATH or (b) RUNPATH within the program itself or a referenced library. NOTE: this issue exists because of an incorrect fix for CVE-2010-3847.

CVE-2011-2702

MEDIUM SEVERITY	Integer signedness error in Glibc before 2.13 and eglibc before 2.13, when using Supplemental Streaming SIMD Extensions 3 (SSSE3) optimization, allows context-

	dependent attackers to execute arbitrary code via a negative length parameter to (1) memcpy-ssse3-rep.S, (2) memcpy-ssse3.S, or (3) memset-sse2.S in sysdeps/i386 /i686/multiarch/, which triggers an out-of-bounds read, as demonstrated using the memcpy function.
CVE-2015-7547	
MEDIUM SEVERITY	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.
CVE-2015-1781	
MEDIUM SEVERITY	Buffer overflow in the gethostbyname_r and other unspecified NSS functions in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response, which triggers a call with a misaligned buffer.

CVE-2015-8776

MEDIUM SEVERITY

The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.

CVE-2015-5229

MEDIUM SEVERITY

The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly initialize memory areas, which might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.

CVE-2010-4052

MEDIUM SEVERITY

Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.

CVE-2010-4051

MEDIUM SEVERITY	The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."

CVE-2016-1234

MEDIUM SEVERITY	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.

CVE-2014-8121

MEDIUM SEVERITY	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up on a database while iterating over it, which triggers the file pointer to be reset.

CVE-2009-0537

MEDIUM SEVERITY

Integer overflow in the fts_build function in fts.c in libc in (1) OpenBSD 4.4 and earlier and (2) Microsoft Interix 6.0 build 10.0.6030.0 allows context-dependent attackers to cause a denial of service (application crash) via a deep directory tree, related to the fts_level structure member, as demonstrated by (a) du, (b) rm, (c) chmod, and (d) chgrp on OpenBSD; and (e) SearchIndexer.exe on Vista Enterprise.

CVE-2010-4756

MEDIUM SEVERITY

The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.

CVE-2013-2207

LOW SEVERITY

pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-

	terminals by leveraging a FUSE file system.
CVE-2015-8777	
LOW SEVERITY	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.

libcurl3-gnutls	**7.38.0**
CVE-2015-3144	
HIGH SEVERITY	The fix_hostname function in cURL and libcurl 7.37.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) or possibly have other unspecified impact via a zero-length host name, as demonstrated by "http://:80" and ":80."
CVE-2015-3145	
HIGH SEVERITY	The sanitize_cookie_path function in cURL and libcurl 7.31.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds write and crash) or possibly have

	other unspecified impact via a cookie path containing only a double-quote character.
CVE-2015-3237	
MEDIUM SEVERITY	The smb_request_state function in cURL and libcurl 7.40.0 through 7.42.1 allows remote SMB servers to obtain sensitive information from memory or cause a denial of service (out-of-bounds read and crash) via crafted length and offset values.
CVE-2014-8151	
MEDIUM SEVERITY	The darwinssl_connect_step1 function in lib/vtls/curl_darwinssl.c in libcurl 7.31.0 through 7.39.0, when using the DarwinSSL (aka SecureTransport) back-end for TLS, does not check if a cached TLS session validated the certificate when reusing the session, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.
CVE-2010-3842	
MEDIUM SEVERITY	Absolute path traversal vulnerability in curl 7.20.0 through 7.21.1, when the --remote-header-name or -J option is used, allows remote servers to create or overwrite arbitrary files by using \ (backslash) as a separator of path components within the Content-disposition HTTP header.

CVE-2015-3143

MEDIUM SEVERITY

cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0015.

CVE-2015-3153

MEDIUM SEVERITY

The default configuration for cURL and libcurl before 7.42.1 sends custom HTTP headers to both the proxy and destination server, which might allow remote proxy servers to obtain sensitive information by reading the header contents.

CVE-2016-0755

MEDIUM SEVERITY

The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated proxy connections, which might allow remote attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015.

CVE-2016-0754

MEDIUM SEVERITY

cURL before 7.47.0 on Windows allows attackers to write to arbitrary files in the current working directory on a different drive via a colon in a remote file name.

CVE-2015-3148

MEDIUM SEVERITY

cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

CVE-2015-3236

MEDIUM SEVERITY

cURL and libcurl 7.40.0 through 7.42.1 sends the HTTP Basic authentication credentials for a previous connection when reusing a reset (curl_easy_reset) connection handle to send a request to the same host name, which allows remote attackers to obtain sensitive information via unspecified vectors.

CVE-2014-3707

MEDIUM SEVERITY

The curl_easy_duphandle function in libcurl 7.17.1 through 7.38.0, when running with the CURLOPT_COPYPOSTFIELDS option, does not properly copy HTTP POST data for an easy handle, which triggers an out-of-bounds read that allows remote web servers to read sensitive memory information.

CVE-2014-1263

MEDIUM SEVERITY

curl and libcurl 7.27.0 through 7.35.0, when using the SecureTransport/Darwinssl backend, as used in in Apple OS X 10.9.x

	before 10.9.2, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate when accessing a URL that uses a numerical IP address, which allows man-in-the-middle attackers to spoof servers via an arbitrary valid certificate.
CVE-2014-8150	
MEDIUM SEVERITY	CRLF injection vulnerability in libcurl 6.0 through 7.x before 7.40.0, when using an HTTP proxy, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in a URL.
CVE-2014-2522	
MEDIUM SEVERITY	curl and libcurl 7.27.0 through 7.35.0, when runnning on Windows and using the SChannel/Winssl TLS backend, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate when accessing a URL that uses a numerical IP address, which allows man-in-the-middle attackers to spoof servers via an arbitrary valid certificate.
CVE-2016-3739	

LOW SEVERITY	The (1) mbed_connect_step1 function in lib/vtls/mbedtls.c and (2) polarssl_connect_step1 function in lib/vtls /polarssl.c in cURL and libcurl before 7.49.0, when using SSLv3 or making a TLS connection to a URL that uses a numerical IP address, allow remote attackers to spoof servers via an arbitrary valid certificate.

libgnutls11	**3.3.8**
CVE-2015-3308	
HIGH SEVERITY	Double free vulnerability in lib/x509/x509_ext.c in GnuTLS before 3.3.14 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted CRL distribution point.
CVE-2009-5138	
MEDIUM SEVERITY	GnuTLS before 2.7.6, when the GNUTLS_VERIFY_ALLOW_X509_V1_CA_CRT flag is not enabled, treats version 1 X.509 certificates as intermediate CAs, which allows remote attackers to bypass intended restrictions by leveraging a X.509 V1 certificate from a trusted CA to issue new certificates, a different vulnerability than CVE-2014-1959.

CVE-2015-0282

MEDIUM SEVERITY

GnuTLS before 3.1.0 does not verify that the RSA PKCS #1 signature algorithm matches the signature algorithm in the certificate, which allows remote attackers to conduct downgrade attacks via unspecified vectors.

CVE-2013-4466

MEDIUM SEVERITY

Buffer overflow in the dane_query_tlsa function in the DANE library (libdane) in GnuTLS 3.1.x before 3.1.15 and 3.2.x before 3.2.5 allows remote servers to cause a denial of service (memory corruption) via a response with more than four DANE entries.

CVE-2013-4487

MEDIUM SEVERITY

Off-by-one error in the dane_raw_tlsa in the DANE library (libdane) in GnuTLS 3.1.x before 3.1.16 and 3.2.x before 3.2.6 allows remote servers to cause a denial of service (memory corruption) via a response with more than four DANE entries. NOTE: this issue is due to an incomplete fix for CVE-2013-4466.

CVE-2015-6251

MEDIUM SEVERITY

Double free vulnerability in GnuTLS before 3.3.17 and 3.4.x before 3.4.4 allows remote attackers to cause a denial of service via a long

	DistinguishedName (DN) entry in a certificate.
CVE-2014-8155	
MEDIUM SEVERITY	GnuTLS before 2.9.10 does not verify the activation and expiration dates of CA certificates, which allows man-in-the-middle attackers to spoof servers via a certificate issued by a CA certificate that is (1) not yet valid or (2) no longer valid.
CVE-2011-3389	
MEDIUM SEVERITY	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE-2015-7575	
MEDIUM SEVERITY	Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x before 38.5.2, does not

	reject MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it easier for man-in-the-middle attackers to spoof servers by triggering a collision.

libjpeg	**1.3.1**
CVE-2012-2806	
MEDIUM SEVERITY	Heap-based buffer overflow in the get_sos function in jdmarker.c in libjpeg-turbo 1.2.0 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a large component count in the header of a JPEG image.

libpng	**1.2.50**
CVE-2014-9495	
HIGH SEVERITY	Heap-based buffer overflow in the png_combine_row function in libpng before 1.5.21 and 1.6.x before 1.6.16, when running on 64-bit systems, might allow context-dependent attackers to execute arbitrary code via a "very wide interlaced" PNG image.

CVE-2015-8540

HIGH SEVERITY

Integer underflow in the png_check_keyword function in pngwutil.c in libpng 0.90 through 0.99, 1.0.x before 1.0.66, 1.1.x and 1.2.x before 1.2.56, 1.3.x and 1.4.x before 1.4.19, and 1.5.x before 1.5.26 allows remote attackers to have unspecified impact via a space character as a keyword in a PNG image, which triggers an out-of-bounds read.

CVE-2011-3464

HIGH SEVERITY

Off-by-one error in the png_formatted_warning function in pngerror.c in libpng 1.5.4 through 1.5.7 might allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unspecified vectors, which trigger a stack-based buffer overflow.

CVE-2015-8472

HIGH SEVERITY

Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in

	a PNG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8126.
CVE-2015-0973	
HIGH SEVERITY	Buffer overflow in the png_read_IDAT_data function in pngrutil.c in libpng before 1.5.21 and 1.6.x before 1.6.16 allows context-dependent attackers to execute arbitrary code via IDAT data with a large width, a different vulnerability than CVE-2014-9495.
CVE-2015-8126	
HIGH SEVERITY	Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.
CVE-2011-0408	
MEDIUM SEVERITY	pngrtran.c in libpng 1.5.x before 1.5.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted palette-based

	PNG image that triggers a buffer overflow, related to the png_do_expand_palette function, the png_do_rgb_to_gray function, and an integer underflow. NOTE: some of these details are obtained from third party information.
CVE-2013-7354	
MEDIUM SEVERITY	Multiple integer overflows in libpng before 1.5.14rc03 allow remote attackers to cause a denial of service (crash) via a crafted image to the (1) png_set_sPLT or (2) png_set_text_2 function, which triggers a heap-based buffer overflow.
CVE-2013-7353	
MEDIUM SEVERITY	Integer overflow in the png_set_unknown_chunks function in libpng/pngset.c in libpng before 1.5.14beta08 allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a crafted image, which triggers a heap-based buffer overflow.
CVE-2014-0333	
MEDIUM SEVERITY	The png_push_read_chunk function in pngpread.c in the progressive decoder in libpng 1.6.x through 1.6.9 allows remote attackers to cause a denial of service (infinite

	loop and CPU consumption) via an IDAT chunk with a length of zero.
CVE-2013-6954	
MEDIUM SEVERITY	The png_do_expand_palette function in libpng before 1.6.8 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via (1) a PLTE chunk of zero bytes or (2) a NULL palette, related to pngrtran.c and pngset.c.
CVE-2015-7981	
MEDIUM SEVERITY	The png_convert_to_rfc1123 function in png.c in libpng 1.0.x before 1.0.64, 1.2.x before 1.2.54, and 1.4.x before 1.4.17 allows remote attackers to obtain sensitive process memory information via crafted tIME chunk data in an image file, which triggers an out-of-bounds read.
CVE-2007-5268	
MEDIUM SEVERITY	pngrtran.c in libpng before 1.0.29 and 1.2.x before 1.2.21 use (1) logical instead of bitwise operations and (2) incorrect comparisons, which might allow remote attackers to cause a denial of service (crash) via a crafted PNG image.
CVE-2007-5266	

MEDIUM SEVERITY	Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.0.29 beta1 and 1.2.x before 1.2.21 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image that prevents a name field from being NULL terminated.
CVE-2007-5267	
MEDIUM SEVERITY	Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.2.22 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image, due to an incorrect fix for CVE-2007-5266.
CVE-2011-3328	
LOW SEVERITY	The png_handle_cHRM function in pngrutil.c in libpng 1.5.4, when color-correction support is enabled, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a malformed PNG image containing a cHRM chunk associated with a certain zero value.

libstdc++6	**4.9.2**
CVE-2015-5276	

MEDIUM SEVERITY	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not properly handle short reads from blocking sources, which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.

libxml2	**2.9.1+dfsg1**
CVE-2016-1762	
HIGH SEVERITY	libxml2 in Apple iOS before 9.3, OS X before 10.11.4, Safari before 9.1, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2013-1969	
HIGH SEVERITY	Multiple use-after-free vulnerabilities in libxml2 2.9.0 and possibly other versions might allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to the (1) htmlParseChunk and (2) xmldecl_done functions, as demonstrated by a buffer overflow in the xmlBufGetInputBase function.

CVE-2015-8710

HIGH SEVERITY

The htmlParseComment function in HTMLparser.c in libxml2 allows attackers to obtain sensitive information, cause a denial of service (out-of-bounds heap memory access and application crash), or possibly have unspecified other impact via an unclosed HTML comment.

CVE-2015-5312

HIGH SEVERITY

The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.

CVE-2016-1840

MEDIUM SEVERITY

libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1839.

CVE-2015-7942

MEDIUM SEVERITY

The xmlParseConditionalSections function in parser.c in libxml2 does not properly skip intermediary entities when it stops parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted XML data, a different vulnerability than CVE-2015-7941.

CVE-2016-1834

MEDIUM SEVERITY

libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.

CVE-2016-1833

MEDIUM SEVERITY

libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838,

	CVE-2016-1839, and CVE-2016-1840.
CVE-2016-1838	
MEDIUM SEVERITY	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1839, and CVE-2016-1840.
CVE-2016-1837	
MEDIUM SEVERITY	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.
CVE-2016-1836	
MEDIUM SEVERITY	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of

	service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.
CVE-2016-1835	
MEDIUM SEVERITY	libxml2, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1839	
MEDIUM SEVERITY	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1840.
CVE-2015-8241	
MEDIUM SEVERITY	The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to cause a denial of service (heap-based buffer over-read

	and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8242	
MEDIUM SEVERITY	The xmlSAX2TextNode function in SAX2.c in the push interface in the HTML parser in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (stack-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8806	
MEDIUM SEVERITY	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "
CVE-2015-1819	
MEDIUM SEVERITY	The xmlreader in libxml allows remote attackers to cause a denial of service (memory consumption) via crafted XML data, related to an XML Entity Expansion (XEE) attack.
CVE-2016-3627	
MEDIUM SEVERITY	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent

	attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2015-7497	
MEDIUM SEVERITY	Heap-based buffer overflow in the xmlDictComputeFastQKey function in dict.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors.
CVE-2015-7499	
MEDIUM SEVERITY	Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive process memory information via unspecified vectors.
CVE-2016-3705	
MEDIUM SEVERITY	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2015-7498	

MEDIUM SEVERITY	Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors related to extracting errors after an encoding conversion failure.

CVE-2015-8317

MEDIUM SEVERITY	The xmlParseXMLDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive information via an (1) unterminated encoding value or (2) incomplete XML declaration in XML data, which triggers an out-of-bounds heap read.

CVE-2008-4409

MEDIUM SEVERITY	libxml2 2.7.0 and 2.7.1 does not properly handle "predefined entities definitions" in entities, which allows context-dependent attackers to cause a denial of service (memory consumption and application crash), as demonstrated by use of xmllint on a certain XML document, a different vulnerability than CVE-2003-1564 and CVE-2008-3281.

CVE-2015-7500

MEDIUM SEVERITY	The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (out-of-

	bounds heap read) via unspecified vectors related to incorrect entities boundaries and start tags.
CVE-2016-2073	
MEDIUM SEVERITY	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.
CVE-2015-7941	
MEDIUM SEVERITY	libxml2 2.9.2 does not properly stop parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and libxml2 crash) via crafted XML data to the (1) xmlParseEntityDecl or (2) xmlParseConditionalSections function in parser.c, as demonstrated by non-terminated entities.
CVE-2015-8035	
LOW SEVERITY	The xz_decomp function in xzlib.c in libxml2 2.9.1 does not properly detect compression errors, which allows context-dependent attackers to cause a denial of service (process hang) via crafted XML data.

mount	**2.25.2**

CVE-2015-5218	
LOW SEVERITY	Buffer overflow in text-utils/colcrt.c in colcrt in util-linux before 2.27 allows local users to cause a denial of service (crash) via a crafted file, related to the page global variable.
CVE-2007-0822	
LOW SEVERITY	umount, when running with the Linux 2.6.15 kernel on Slackware Linux 10.2, allows local users to trigger a NULL dereference and application crash by invoking the program with a pathname for a USB pen drive that was mounted and then physically removed, which might allow the users to obtain sensitive information, including core file contents.

OpenLDAP	**2.4.40+dfsg**
CVE-2015-3276	
MEDIUM SEVERITY	The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.

CVE-2015-6908

MEDIUM SEVERITY

The ber_get_next function in libraries/liblber/io.c in OpenLDAP 2.4.42 and earlier allows remote attackers to cause a denial of service (reachable assertion and application crash) via crafted BER data, as demonstrated by an attack against slapd.

CVE-2012-2668

MEDIUM SEVERITY

libraries/libldap/tls_m.c in OpenLDAP, possibly 2.4.31 and earlier, when using the Mozilla NSS backend, always uses the default cipher suite even when TLSCipherSuite is set, which might cause OpenLDAP to use weaker ciphers than intended and make it easier for remote attackers to obtain sensitive information.

OpenSSL **1.0.1e**

CVE-2016-2108

HIGH SEVERITY

The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

CVE-2016-0799

HIGH SEVERITY

The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.

CVE-2016-2842

HIGH SEVERITY

The doapr_outch function in crypto/bio /b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.

CVE-2016-0705

HIGH SEVERITY

Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have

	unspecified other impact via a malformed DSA private key.
CVE-2016-2109	
HIGH SEVERITY	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
CVE-2016-0798	
HIGH SEVERITY	Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.
CVE-2010-4252	
HIGH SEVERITY	OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

CVE-2012-2131

HIGH SEVERITY

Multiple integer signedness errors in crypto/buffer/buffer.c in OpenSSL 0.9.8v allow remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2110.

CVE-2010-1378

HIGH SEVERITY

OpenSSL in Apple Mac OS X 10.6.x before 10.6.5 does not properly perform arithmetic, which allows remote attackers to bypass X.509 certificate authentication via an arbitrary certificate issued by a legitimate Certification Authority.

CVE-2014-8176

HIGH SEVERITY

The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via

	unexpected application data.
CVE-2015-0292	
HIGH SEVERITY	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.
CVE-2014-3512	
HIGH SEVERITY	Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.
CVE-2014-3567	
HIGH SEVERITY	Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.
CVE-2014-3513	

HIGH SEVERITY	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.

CVE-2014-3509

MEDIUM SEVERITY	Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.

CVE-2015-0209

MEDIUM SEVERITY	Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec /ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

CVE-2014-0195

MEDIUM SEVERITY

The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

CVE-2014-0224

MEDIUM SEVERITY

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

CVE-2015-1791

MEDIUM SEVERITY

Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded

client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

CVE-2014-2234

MEDIUM SEVERITY

A certain Apple patch for OpenSSL in Apple OS X 10.9.2 and earlier uses a Trust Evaluation Agent (TEA) feature without terminating certain TLS/SSL handshakes as specified in the SSL_CTX_set_verify callback function's documentation, which allows remote attackers to bypass extra verification within a custom application via a crafted certificate chain that is acceptable to TEA but not acceptable to that application.

CVE-2016-2176

MEDIUM SEVERITY

The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

CVE-2015-1793

MEDIUM SEVERITY	The X509_verify_cert function in crypto/x509 /x509_vfy.c in OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c does not properly process X.509 Basic Constraints cA values during identification of alternative certificate chains, which allows remote attackers to spoof a Certification Authority role and trigger unintended certificate verifications via a valid leaf certificate.

CVE-2010-1633

MEDIUM SEVERITY	RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and possibly other applications, returns uninitialized memory upon failure, which might allow context-dependent attackers to bypass intended key requirements or obtain sensitive information via unspecified vectors. NOTE: some of these details are obtained from third party information.

CVE-2013-6450

MEDIUM SEVERITY	The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by

	interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.
CVE-2007-6755	
MEDIUM SEVERITY	The NIST SP 800-90A default statement of the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm contains point Q constants with a possible relationship to certain "skeleton key" values, which might allow context-dependent attackers to defeat cryptographic protection mechanisms by leveraging knowledge of those values. NOTE: this is a preliminary CVE for Dual_EC_DRBG; future research may provide additional details about point Q and associated attacks, and could potentially lead to a RECAST or REJECT of this CVE.
CVE-2014-3507	
MEDIUM SEVERITY	Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.
CVE-2014-3505	

MEDIUM SEVERITY	Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

CVE-2014-3506

MEDIUM SEVERITY	d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

CVE-2015-3195

MEDIUM SEVERITY	The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2015-3194

MEDIUM	crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before

SEVERITY	1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3193

MEDIUM SEVERITY	The Montgomery squaring implementation in crypto/bn/asm/x86_64-mont5.pl in OpenSSL 1.0.2 before 1.0.2e on the x86_64 platform, as used by the BN_mod_exp function, mishandles carry propagation and produces incorrect output, which makes it easier for remote attackers to obtain sensitive private-key information via an attack against use of a (1) Diffie-Hellman (DH) or (2) Diffie-Hellman Ephemeral (DHE) ciphersuite.

CVE-2014-8275

MEDIUM SEVERITY	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1 /a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa /ecs_vrf.c, and crypto/x509/x_all.c.

CVE-2015-0206

MEDIUM SEVERITY	Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.

CVE-2015-0207

MEDIUM SEVERITY	The dtls1_listen function in d1_lib.c in OpenSSL 1.0.2 before 1.0.2a does not properly isolate the state information of independent data streams, which allows remote attackers to cause a denial of service (application crash) via crafted DTLS traffic, as demonstrated by DTLS 1.0 traffic to a DTLS 1.2 server.

CVE-2015-0205

MEDIUM SEVERITY	The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.

CVE-2015-0288

MEDIUM SEVERITY	The X509_to_X509_REQ function in crypto/x509 /x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

CVE-2015-0289

MEDIUM SEVERITY	The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7 /pk7_lib.c.

CVE-2015-0286

MEDIUM SEVERITY	The ASN1_TYPE_cmp function in crypto/asn1 /a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint

	that uses the certificate-verification feature.
CVE-2015-0287	
MEDIUM SEVERITY	The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.
CVE-2009-0789	
MEDIUM SEVERITY	OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.
CVE-2016-2106	
MEDIUM SEVERITY	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of

	data.
CVE-2014-3572	
MEDIUM SEVERITY	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.
CVE-2014-3570	
MEDIUM SEVERITY	The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn /asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.
CVE-2014-3571	
MEDIUM SEVERITY	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the

	ssl3_read_n function in s3_pkt.c.
CVE-2016-2105	
MEDIUM SEVERITY	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
CVE-2015-1792	
MEDIUM SEVERITY	The do_free_upto function in crypto/cms /cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.
CVE-2015-1790	
MEDIUM SEVERITY	The PKCS7_dataDecodefunction in crypto/pkcs7 /pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

CVE-2014-3569

MEDIUM SEVERITY

The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.

CVE-2016-0797

MEDIUM SEVERITY

Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.

CVE-2015-1794

MEDIUM SEVERITY

The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a denial of service (segmentation fault) via a zero p value in an anonymous Diffie-Hellman (DH)

	ServerKeyExchange message.
CVE-2015-0293	
MEDIUM SEVERITY	The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.
CVE-2015-0291	
MEDIUM SEVERITY	The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.
CVE-2015-0290	
MEDIUM SEVERITY	The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.

CVE-2014-0160

MEDIUM SEVERITY

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

CVE-2015-0285

MEDIUM SEVERITY

The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.

CVE-2014-3508

MEDIUM SEVERITY

The OBJ_obj2txt function in crypto/objects /obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline,

	X509_name_print_ex, and unspecified other functions.
CVE-2015-3197	
MEDIUM SEVERITY	ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.
CVE-2015-3196	
MEDIUM SEVERITY	ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted ServerKeyExchange message.
CVE-2014-0198	
MEDIUM SEVERITY	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL

	pointer dereference and application crash) via vectors that trigger an alert condition.
CVE-2014-0076	
MEDIUM SEVERITY	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.
CVE-2013-4353	
MEDIUM SEVERITY	The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.
CVE-2015-0208	
MEDIUM SEVERITY	The ASN.1 signature-verification implementation in the rsa_item_verify function in crypto/rsa/rsa_ameth.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted RSA PSS parameters to an endpoint that uses the certificate-verification feature.

CVE-2015-0204

MEDIUM SEVERITY

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

CVE-2015-4000

MEDIUM SEVERITY

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

CVE-2014-0221

MEDIUM SEVERITY

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service

	(recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.
CVE-2016-0800	
MEDIUM SEVERITY	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.
CVE-2014-3566	
MEDIUM SEVERITY	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
CVE-2014-3568	
MEDIUM SEVERITY	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

CVE-2015-3216

MEDIUM SEVERITY

Race condition in a certain Red Hat patch to the PRNG lock implementation in the ssleay_rand_bytes function in OpenSSL, as distributed in openssl-1.0.1e-25.el7 in Red Hat Enterprise Linux (RHEL) 7 and other products, allows remote attackers to cause a denial of service (application crash) by establishing many TLS sessions to a multithreaded server, leading to use of a negative value for a certain length field.

CVE-2015-7575

MEDIUM SEVERITY

Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x before 38.5.2, does not reject MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it easier for man-in-the-middle attackers to spoof servers by triggering a collision.

CVE-2010-0433

MEDIUM SEVERITY

The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer

	dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.
CVE-2014-3510	
MEDIUM SEVERITY	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.
CVE-2014-5139	
MEDIUM SEVERITY	The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.
CVE-2014-3511	
MEDIUM SEVERITY	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message

	fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.
CVE-2014-3470	
MEDIUM SEVERITY	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.
CVE-2013-6449	
MEDIUM SEVERITY	The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.
CVE-2015-1788	
MEDIUM SEVERITY	The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field,

	which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.
CVE-2016-0704	
MEDIUM SEVERITY	An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.
CVE-2015-1789	
MEDIUM SEVERITY	The X509_cmp_time function in crypto/x509 /x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

CVE-2016-0703

MEDIUM SEVERITY

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2010-0928

MEDIUM SEVERITY

OpenSSL 0.9.8i on the Gaisler Research LEON3 SoC on the Xilinx Virtex-II Pro FPGA uses a Fixed Width Exponentiation (FWE) algorithm for certain signature calculations, and does not verify the signature before providing it to a caller, which makes it easier for physically proximate attackers to determine the private key via a modified supply voltage for the microprocessor, related to a "fault-based attack."

CVE-2010-5298

MEDIUM SEVERITY

Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled,

	allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.
CVE-2016-2107	
LOW SEVERITY	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.
CVE-2012-4929	
LOW SEVERITY	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
CVE-2009-0591	
LOW	The CMS_verify function in OpenSSL 0.9.8h

SEVERITY	through 0.9.8j, when CMS is enabled, does not properly handle errors associated with malformed signed attributes, which allows remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid.

CVE-2016-0701

LOW SEVERITY	The DH_check_pub_key function in crypto/dh /dh_check.c in OpenSSL 1.0.2 before 1.0.2f does not ensure that prime numbers are appropriate for Diffie-Hellman (DH) key exchange, which makes it easier for remote attackers to discover a private DH exponent by making multiple handshakes with a peer that chose an inappropriate number, as demonstrated by a number in an X9.42 file.

CVE-2015-1787

LOW SEVERITY	The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.

CVE-2016-0702

LOW	The MOD_EXP_CTIME_COPY_FROM_PREBUF

SEVERITY	function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack.

pam	**1.1.8**
CVE-2007-0003	
HIGH SEVERITY	pam_unix.so in Linux-PAM 0.99.7.0 allows context-dependent attackers to log into accounts whose password hash, as stored in /etc/passwd or /etc/shadow, has only two characters.
CVE-2010-0832	
MEDIUM SEVERITY	pam_motd (aka the MOTD module) in libpam-modules before 1.1.0-2ubuntu1.1 in PAM on Ubuntu 9.10 and libpam-modules before 1.1.1-2ubuntu5 in PAM on Ubuntu 10.04 LTS allows local users to change the ownership of arbitrary files via a symlink attack on .cache in a user's home directory, related to "user file stamps" and the motd.legal-notice file.

CVE-2014-2583	
MEDIUM SEVERITY	Multiple directory traversal vulnerabilities in pam_timestamp.c in the pam_timestamp module for Linux-PAM (aka pam) 1.1.8 allow local users to create aribitrary files or possibly bypass authentication via a .. (dot dot) in the (1) PAM_RUSER value to the get_ruser function or (2) PAM_TTY value to the check_tty funtion, which is used by the format_timestamp_name function.
CVE-2015-3238	
MEDIUM SEVERITY	The _unix_run_helper_binary function in the pam_unix module in Linux-PAM (aka pam) before 1.2.1, when unable to directly access passwords, allows local users to enumerate usernames or cause a denial of service (hang) via a large password.
CVE-2003-0388	
MEDIUM SEVERITY	pam_wheel in Linux-PAM 0.78, with the trust option enabled and the use_uid option disabled, allows local users to spoof log entries and gain privileges by causing getlogin() to return a spoofed user name.

PCRE	**10.21**

CVE-2016-3191

HIGH SEVERITY

The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39 and pcre2_compile.c in PCRE2 before 10.22 mishandles patterns containing an (*ACCEPT) substring in conjunction with nested parentheses, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, aka ZDI-CAN-3542.

CVE-2015-8380

HIGH SEVERITY

The pcre_exec function in pcre_exec.c in PCRE before 8.38 mishandles a // pattern with a \01 string, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.

CVE-2016-1283

HIGH SEVERITY

The pcre_compile2 function in pcre_compile.c in PCRE 8.38 mishandles the /((?:F?+(?:^(?(R)a+\"){99}-))(?J)(?'R'(?'R'<((?'RR'(?'R'\){97)?J)?J)(?'R'(?'R'\){99|(:(?|(?'R')(\k'R')|((?'R')))H'R'R)

	(H'R))))))/ pattern and related patterns with named subgroups, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.

Perl	**5.20.2**
CVE-2004-0377	
HIGH SEVERITY	Buffer overflow in the win32_stat function for (1) ActiveState's ActivePerl and (2) Larry Wall's Perl before 5.8.3 allows local or remote attackers to execute arbitrary commands via filenames that end in a backslash character.
CVE-2015-8607	
HIGH SEVERITY	The canonpath function in the File::Spec module in PathTools before 3.62, as used in Perl, does not properly preserve the taint attribute of data, which might allow context-dependent attackers to bypass the taint protection mechanism via a crafted string.
CVE-2005-4217	

HIGH SEVERITY	Perl in Apple Mac OS X Server 10.3.9 does not properly drop privileges when using the "$<" variable to set uid, which allows attackers to gain privileges.
CVE-2005-4278	
HIGH SEVERITY	Untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.
CVE-2015-8853	
MEDIUM SEVERITY	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by "a\x80."
CVE-2016-2381	
MEDIUM SEVERITY	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in envp.
CVE-2010-1158	

MEDIUM SEVERITY	Integer overflow in the regular expression engine in Perl 5.8.x allows context-dependent attackers to cause a denial of service (stack consumption and application crash) by matching a crafted regular expression against a long string.

perl-base	**5.20.2**
CVE-2004-0377	
HIGH SEVERITY	Buffer overflow in the win32_stat function for (1) ActiveState's ActivePerl and (2) Larry Wall's Perl before 5.8.3 allows local or remote attackers to execute arbitrary commands via filenames that end in a backslash character.
CVE-2015-8607	
HIGH SEVERITY	The canonpath function in the File::Spec module in PathTools before 3.62, as used in Perl, does not properly preserve the taint attribute of data, which might allow context-dependent attackers to bypass the taint protection mechanism via a crafted string.
CVE-2005-4217	
HIGH SEVERITY	Perl in Apple Mac OS X Server 10.3.9 does not properly drop privileges when using the

	"$<" variable to set uid, which allows attackers to gain privileges.
CVE-2005-4278	
HIGH SEVERITY	Untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.
CVE-2015-8853	
MEDIUM SEVERITY	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by "a\x80."
CVE-2016-2381	
MEDIUM SEVERITY	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in envp.
CVE-2010-1158	
MEDIUM SEVERITY	Integer overflow in the regular expression engine in Perl 5.8.x allows context-

	dependent attackers to cause a denial of service (stack consumption and application crash) by matching a crafted regular expression against a long string.

php5-dev	**5.6.21+dfsg**
CVE-2015-4642	
HIGH SEVERITY	The escapeshellarg function in ext/standard /exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.
CVE-2012-2376	
HIGH SEVERITY	Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.
CVE-2007-2844	
HIGH SEVERITY	PHP 4.x and 5.x before 5.2.1, when running on multi-threaded systems, does not ensure

	thread safety for libc crypt function calls using protection schemes such as a mutex, which creates race conditions that allow remote attackers to overwrite internal program memory and gain system access.
CVE-2007-5653	
HIGH SEVERITY	The Component Object Model (COM) functions in PHP 5.x on Windows do not follow safe_mode and disable_functions restrictions, which allows context-dependent attackers to bypass intended limitations, as demonstrated by executing objects with the kill bit set in the corresponding ActiveX control Compatibility Flags, executing programs via a function in compatUI.dll, invoking wscript.shell via wscript.exe, invoking Scripting.FileSystemObject via wshom.ocx, and adding users via a function in shgina.dll, related to the com_load_typelib function.
CVE-2007-1412	
HIGH SEVERITY	The cpdf_open function in the ClibPDF (cpdf) extension in PHP 4.4.6 allows context-dependent attackers to obtain sensitive information (script source code) via a long string in the second argument.
CVE-2007-1381	

HIGH SEVERITY	The wddx_deserialize function in wddx.c 1.119.2.10.2.12 and 1.119.2.10.2.13 in PHP 5, as modified in CVS on 20070224 and fixed on 20070304, calls strlcpy where strlcat was intended and uses improper arguments, which allows context-dependent attackers to execute arbitrary code via a WDDX packet with a malformed overlap of a STRING element, which triggers a buffer overflow.

CVE-2015-6527

HIGH SEVERITY	The php_str_replace_in_subject function in ext/standard/string.c in PHP 7.x before 7.0.0 allows remote attackers to execute arbitrary code via a crafted value in the third argument to the str_ireplace function.

CVE-2008-5844

HIGH SEVERITY	PHP 5.2.7 contains an incorrect change to the FILTER_UNSAFE_RAW functionality, and unintentionally disables magic_quotes_gpc regardless of the actual magic_quotes_gpc setting, which might make it easier for context-dependent attackers to conduct SQL injection attacks and unspecified other attacks.

CVE-2008-0674

HIGH SEVERITY	Buffer overflow in PCRE before 7.6 allows remote attackers to execute arbitrary code via

	a regular expression containing a character class with a large number of characters with Unicode code points greater than 255.
CVE-2006-0097	
HIGH SEVERITY	Stack-based buffer overflow in the create_named_pipe function in libmysql.c in PHP 4.3.10 and 4.4.x before 4.4.3 for Windows allows attackers to execute arbitrary code via a long (1) arg_host or (2) arg_unix_socket argument, as demonstrated by a long named pipe variable in the host argument to the mysql_connect function.
CVE-2014-9425	
HIGH SEVERITY	Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1904	
HIGH SEVERITY	Multiple integer overflows in ext/standard /exec.c in PHP 7.x before 7.0.2 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a long string to the (1) php_escape_shell_cmd or

	(2) php_escape_shell_arg function, leading to a heap-based buffer overflow.
CVE-2016-3074	
HIGH SEVERITY	Integer signedness error in GD Graphics Library 2.1.1 (aka libgd or libgd2) allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via crafted compressed gd2 data, which triggers a heap-based buffer overflow.
CVE-2009-3293	
HIGH SEVERITY	Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."
CVE-2007-1411	
MEDIUM SEVERITY	Buffer overflow in PHP 4.4.6 and earlier, and unspecified PHP 5 versions, allows local and possibly remote attackers to execute arbitrary code via long server name arguments to the (1) mssql_connect and (2) mssql_pconnect functions.
CVE-2007-4010	
MEDIUM	The win32std extension in PHP 5.2.3 does not

SEVERITY	follow safe_mode and disable_functions restrictions, which allows remote attackers to execute arbitrary commands via the win_shell_execute function.

CVE-2010-4700

MEDIUM SEVERITY	The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when the MySQLi extension is used, does not properly interact with use of the mysqli_fetch_assoc function, which might make it easier for context-dependent attackers to conduct SQL injection attacks via crafted input that had been properly handled in earlier PHP versions.

CVE-2012-5381

MEDIUM SEVERITY	** DISPUTED ** Untrusted search path vulnerability in the installation functionality in PHP 5.3.17, when installed in the top-level C:\ directory, might allow local users to gain privileges via a Trojan horse DLL in the C:\PHP directory, which may be added to the PATH system environment variable by an administrator, as demonstrated by a Trojan horse wlbsctrl.dll file used by the "IKE and AuthIP IPsec Keying Modules" system service in Windows Vista SP1, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 Release Preview. NOTE: CVE disputes this issue

	because the unsafe PATH is established only by a separate administrative action that is not a default part of the PHP installation.
CVE-2007-3790	
MEDIUM SEVERITY	The com_print_typeinfo function in the bz2 extension in PHP 5.2.3 allows context-dependent attackers to cause a denial of service via a long argument.
CVE-2008-4107	
MEDIUM SEVERITY	The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.
CVE-2006-0931	
MEDIUM SEVERITY	Directory traversal vulnerability in PEAR::Archive_Tar 1.2, and other versions before 1.3.2, allows remote attackers to create and overwrite arbitrary files via certain crafted pathnames in a TAR archive.

CVE-2014-9620

MEDIUM SEVERITY

The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of notes.

CVE-2007-1452

MEDIUM SEVERITY

The FDF support (ext/fdf) in PHP 5.2.0 and earlier does not implement the input filtering hooks for ext/filter, which allows remote attackers to bypass web site filters via an application/vnd.fdf formatted POST.

CVE-2008-5498

MEDIUM SEVERITY

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

CVE-2006-4023

MEDIUM SEVERITY

The ip2long function in PHP 5.1.4 and earlier may incorrectly validate an arbitrary string and return a valid network IP address, which allows remote attackers to obtain network information and facilitate other attacks, as demonstrated using SQL injection in the X-FORWARDED-FOR Header in index.php in

	MiniBB 2.0. NOTE: it could be argued that the ip2long behavior represents a risk for security-relevant issues in a way that is similar to strcpy's role in buffer overflows, in which case this would be a class of implementation bugs that would require separate CVE items for each PHP application that uses ip2long in a security-relevant manner.
CVE-2009-3294	
MEDIUM SEVERITY	The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11 and 5.3.x before 5.3.1, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.
CVE-2007-4441	
MEDIUM SEVERITY	Buffer overflow in php_win32std.dll in the win32std extension for PHP 5.2.0 and earlier allows context-dependent attackers to execute arbitrary code via a long string in the filename

	argument to the win_browse_file function.
CVE-2011-0754	
MEDIUM SEVERITY	The SplFileInfo::getType function in the Standard PHP Library (SPL) extension in PHP before 5.3.4 on Windows does not properly detect symbolic links, which might make it easier for local users to conduct symlink attacks by leveraging cross-platform differences in the stat structure, related to lack of a FILE_ATTRIBUTE_REPARSE_POINT check.
CVE-2007-2748	
MEDIUM SEVERITY	The substr_count function in PHP 5.2.1 and earlier allows context-dependent attackers to obtain sensitive information via unspecified vectors, a different affected function than CVE-2007-1375.
CVE-2014-5459	
LOW SEVERITY	The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
CVE-2011-1144	

LOW SEVERITY	The installer in PEAR 1.9.2 and earlier allows local users to overwrite arbitrary files via a symlink attack on the package.xml file, related to the (1) download_dir, (2) cache_dir, (3) tmp_dir, and (4) pear-build-download directories. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-1072.

shadow	**4.2**
CVE-2006-3597	
HIGH SEVERITY	passwd before 1:4.0.13 on Ubuntu 6.06 LTS leaves the root password blank instead of locking it when the administrator selects the "Go Back" option after the final "Installation complete" message and uses the main menu, which causes the password to be zeroed out in the installer's memory.
CVE-2006-1183	
HIGH SEVERITY	The Ubuntu 5.10 installer does not properly clear passwords from the installer log file (questions.dat), and leaves the log file with world-readable permissions, which allows local users to gain privileges.
CVE-2002-1594	

HIGH SEVERITY	Buffer overflow in (1) grpck and (2) pwck, if installed setuid on a system as recommended in some AIX documentation, may allow local users to gain privileges via a long command line argument.
CVE-2007-5686	
MEDIUM SEVERITY	initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.

systemd	**215**
CVE-2013-4392	
LOW SEVERITY	systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.
CVE-2015-8842	
LOW SEVERITY	tmpfiles.d/systemd.conf in systemd before 229 uses weak permissions for /var/log

	/journal/%m/system.journal, which allows local users to obtain sensitive information by reading the file.

The GNU Ada compiler	**1.4.17**
CVE-2008-1688	
HIGH SEVERITY	Unspecified vulnerability in GNU m4 before 1.4.11 might allow context-dependent attackers to execute arbitrary code, related to improper handling of filenames specified with the -F option. NOTE: it is not clear when this issue crosses privilege boundaries.
CVE-2008-1687	
HIGH SEVERITY	The (1) maketemp and (2) mkstemp builtin functions in GNU m4 before 1.4.11 do not quote their output when a file is created, which might allow context-dependent attackers to trigger a macro expansion, leading to unspecified use of an incorrect filename.

udev	**215**
CVE-2013-4392	

LOW SEVERITY	systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.
CVE-2015-8842	
LOW SEVERITY	tmpfiles.d/systemd.conf in systemd before 229 uses weak permissions for /var/log /journal/%m/system.journal, which allows local users to obtain sensitive information by reading the file.

Know Your Code

Black Duck Hub provides the tools you need to quickly find and fix open source vulnerabilities in your code.

Get insight into over 1.5 million open source projects, with early vulnerability reporting and enhanced vulnerability data that goes well beyond NVD.

- Identify open source throughout your code
- Automatically map to known vulnerabilities
- Manage open source use & security policies
- Integrate vulnerbility scanning with CI tools
- Get alerts when new vulnerabilities are reported

See for yourself. Try Black Duck Hub FREE for 14 days.