CVE-2013-0169

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-0169
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-08 19:55:00 UTC
Updated	2023-05-12 12:58:00 UTC
Description	The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other pro

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Oracle	Openjdk	-	All	All	All
Application	Oracle	Openjdk	1.6.0	All	All	All
Application	Oracle	Openjdk	1.6.0	-	All	All
Application	Oracle	Openjdk	1.6.0	update1	All	All
Application	Oracle	Openjdk	1.6.0	update10	All	All
Application	Oracle	Openjdk	1.6.0	update11	All	All
Application	Oracle	Openjdk	1.6.0	update12	All	All
Application	Oracle	Openjdk	1.6.0	update13	All	All
Application	Oracle	Openjdk	1.6.0	update14	All	All
Application	Oracle	Openjdk	1.6.0	update15	All	All
Application	Oracle	Openjdk	1.6.0	update16	All	All
Application	Oracle	Openjdk	1.6.0	update17	All	All
Application	Oracle	Openjdk	1.6.0	update18	All	All
Application	Oracle	Openjdk	1.6.0	update19	All	All

Application	Oracle	Openjdk	1.6.0	update2	All	All
Application	Oracle	Openjdk	1.6.0	update20	All	All
Application	Oracle	Openjdk	1.6.0	update21	All	All
Application	Oracle	Openjdk	1.6.0	update22	All	All
Application	Oracle	Openjdk	1.6.0	update23	All	All
Application	Oracle	Openjdk	1.6.0	update24	All	All
Application	Oracle	Openjdk	1.6.0	update25	All	All
Application	Oracle	Openjdk	1.6.0	update26	All	All
Application	Oracle	Openjdk	1.6.0	update27	All	All
Application	Oracle	Openjdk	1.6.0	update29	All	All
Application	Oracle	Openjdk	1.6.0	update3	All	All
Application	Oracle	Openjdk	1.6.0	update30	All	All
Application	Oracle	Openjdk	1.6.0	update31	All	All
Application	Oracle	Openjdk	1.6.0	update32	All	All
Application	Oracle	Openjdk	1.6.0	update33	All	All
Application	Oracle	Openjdk	1.6.0	update34	All	All
Application	Oracle	Openjdk	1.6.0	update35	All	All
Application	Oracle	Openjdk	1.6.0	update37	All	All
Application	Oracle	Openjdk	1.6.0	update38	All	All
Application	Oracle	Openjdk	1.6.0	update4	All	All
Application	Oracle	Openjdk	1.6.0	update5	All	All
Application	Oracle	Openjdk	1.6.0	update6	All	All
Application	Oracle	Openjdk	1.6.0	update7	All	All
Application	Oracle	Openjdk	1.7.0	All	All	All
Application	Oracle	Openjdk	1.7.0	-	All	All
Application	Oracle	Openjdk	1.7.0	update1	All	All
Application	Oracle	Openjdk	1.7.0	update10	All	All
Application	Oracle	Openjdk	1.7.0	update11	All	All
Application	Oracle	Openjdk	1.7.0	update13	All	All
Application	Oracle	Openjdk	1.7.0	update2	All	All
Application	Oracle	Openjdk	1.7.0	update3	All	All
Application	Oracle	Openjdk	1.7.0	update4	All	All
Application	Oracle	Openjdk	1.7.0	update5	All	All
Application	Oracle	Openjdk	1.7.0	update6	All	All
Application	Oracle	Openjdk	1.7.0	update7	All	All

Application	Oracle	Openjdk	1.7.0	update9	All	All
Application	Oracle	Openjdk	1.8.0	All	All	All
Application	Oracle	Openjdk	-	All	All	All
Application	Oracle	Openjdk	1.6.0	All	All	All
Application	Oracle	Openjdk	1.7.0	All	All	All
Application	Oracle	Openjdk	1.8.0	All	All	All
Application	Polarssl	Polarssl	0.10.0	All	All	All
Application	Polarssl	Polarssl	0.10.1	All	All	All
Application	Polarssl	Polarssl	0.11.0	All	All	All
Application	Polarssl	Polarssl	0.11.1	All	All	All
Application	Polarssl	Polarssl	0.12.0	All	All	All
Application	Polarssl	Polarssl	0.12.1	All	All	All
Application	Polarssl	Polarssl	0.13.1	All	All	All
Application	Polarssl	Polarssl	0.14.0	All	All	All
Application	Polarssl	Polarssl	0.14.2	All	All	All
Application	Polarssl	Polarssl	0.14.3	All	All	All
Application	Polarssl	Polarssl	0.99	pre1	All	All
Application	Polarssl	Polarssl	0.99	pre3	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	1.0.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	rc0	All	All
Application	Polarssl	Polarssl	1.1.0	rc1	All	All
Application	Polarssl	Polarssl	1.1.1	All	All	All
Application	Polarssl	Polarssl	1.1.2	All	All	All
Application	Polarssl	Polarssl	1.1.3	All	All	All
Application	Polarssl	Polarssl	1.1.4	All	All	All
Application	Polarssl	Polarssl	0.10.0	All	All	All
Application	Polarssl	Polarssl	0.10.1	All	All	All
Application	Polarssl	Polarssl	0.11.0	All	All	All
Application	Polarssl	Polarssl	0.11.1	All	All	All
Application	Polarssl	Polarssl	0.12.0	All	All	All
Application	Polarssl	Polarssl	0.12.1	All	All	All
Application	Polarssl	Polarssl	0.13.1	All	All	All

Application	Polarssl	Polarssl	0.14.0	All	All	All
Application	Polarssl	Polarssl	0.14.2	All	All	All
Application	Polarssl	Polarssl	0.14.3	All	All	All
Application	Polarssl	Polarssl	0.99	pre1	All	All
Application	Polarssl	Polarssl	0.99	pre3	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	1.0.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	rc0	All	All
Application	Polarssl	Polarssl	1.1.0	rc1	All	All
Application	Polarssl	Polarssl	1.1.1	All	All	All
Application	Polarssl	Polarssl	1.1.2	All	All	All
Application	Polarssl	Polarssl	1.1.3	All	All	All
Application	Polarssl	Polarssl	1.1.4	All	All	All

References

Reference
Repository / Oval Repository
Red Hat Customer Portal
Java CPU Feb 2013 Update
Red Hat Customer Portal
[security-announce] SUSE-SU-2014:0320-1: critical: Security update for g
Splunk 5.0.3 addresses multiple vulnerabilities - May 28, 2013 | Splunk
Support / Security / Advisories / / MDVSA-2013:095 | Mandriva
Future home of matrixssl.org
Repository / Oval Repository
Oracle Java Multiple Vulnerabilities | US-CERT
APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004
[security-announce] SUSE-SU-2013:0701-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
Security Advisory SA55108 - IBM Tivoli Storage Productivity Center Multiple Vulnerabilities - Secunia
[security-announce] SUSE-SU-2015:0578-1: important: Security update for
[SECURITY] Fedora 18 Update: mingw-openssl-1.0.1e-1.fc18
/err404.html

About Secunia Research | Flexera

PolarSSL 1.2.5 released - Tech Updates

cert-portal.siemens.com/productcert/pdf/ssa-556833.pdf

IBM Security Bulletin: Potential Security Vulnerabilities fixed in IBM WebSphere Application Server 8.0.0.7 - United States

Security Advisory SA53623 - Splunk Cross-Site Scripting and OpenSSL Vulnerabilities - Secunia

Debian -- Security Information -- DSA-2621-1 openssl

About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

'[security bulletin] HPSBUX02857 SSRT101103 rev.1 - HP-UX Running Java, Remote Unauthorized Access, D' - MARC

CVE-2013-0169 | Puppet

'[security bulletin] HPSBMU02874 SSRT101184 rev.1 - HP Service Manager, Java Runtime Environment (JRE' - MARC

Repository / Oval Repository

Security Advisory SA55351 - Oracle Forms and Reports Two Weaknesses - Secunia

[security-announce] openSUSE-SU-2013:0378-1: important: java-1_6_0-openj

'[security bulletin] HPSBUX02856 SSRT101104 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

Red Hat Customer Portal

[security-announce] SUSE-SU-2013:0328-1: important: Security update for

Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities

Red Hat Customer Portal

[security-announce] openSUSE-SU-2016:0640-1: important: Security update

Security Advisory SA55139 - IBM Initiate Master Data Service / InfoSphere Master Data Management OpenSSL Vulnerabilities - Secunia

USN-1735-1: OpenJDK vulnerabilities | Ubuntu

GNU/Andrew's Blog » [SECURITY] IcedTea 2.1.6, 2.2.6 & 2.3.7 for OpenJDK 7 Released!

Support/Advisories/MGASA-2013-0084 - Mageia wiki

'[security bulletin] HPSBOV02852 SSRT101108 rev.1 - HP SSL for OpenVMS, Remote Denial of Service (DoS' - MARC

Multiple TLS And DTLS Implementations CVE-2013-0169 Information Disclosure Vulnerability

Debian -- Security Information -- DSA-2622-1 polarssl

Repository / Oval Repository

Repository / Oval Repository

[security-announce] openSUSE-SU-2013:0375-1: important: java-1_6_0-openj

oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations

Oracle Fusion Middleware Flaws Let Remote Users Deny Service and Partially Access and Modify Data - SecurityTracker

www.isg.rhul.ac.uk/tls/TLStiming.pdf

'[security bulletin] HPSBUX02909 SSRT101289 rev.1 - HP-UX Apache Web Server, Remote Denial of Service' - MARC

[SECURITY] [DLA 1518-1] polarssl security update

Security Advisory SA55350 - Oracle Fusion Middleware Two Information Disclosure Weaknesses - Secunia

Vulnerability Note VU#737740 - Fiery Network Controllers for Xerox DocuColor 242/252/260 Printer/Copier use a vulnerable version of OpenS

Vulnerability Note VU#737740 - Fiery Network Controllers for Xerox DocuColor 242/252/260 Printer/Copier use a vulnerable version of OpenS
Document Display | HPE Support Center
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

591350 General Electric D20MX Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (PRSN-0006)