CVE-2010-5298

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-5298
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-14 22:38:00 UTC
Updated	2022-08-29 20:53:00 UTC
Description	Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUF

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Application	Mariadb	Mariadb	All	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All

Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All

Application	Openssl	Openssl	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All
Application	Openssl	Openssl	0.9.8y	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All

Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All

Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All

Application	Openssl	Openssl	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All
Application	Openssl	Openssl	0.9.8y	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All

Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	-	All	All

References

Reference
kb.bluecoat.com/index
Security Advisory SA59301 - HP Version Control Repository Manager (VCRM) OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA58977 - IBM BladeCenter Advanced Management Module Firmware OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA59162 - McAfee Multiple Products OpenSSL Multiple Vulnerabilities - Secunia
Juniper Networks - Junos Pulse/SA (SSLVPN): Details on fixes for SSL/TLS MITM vulnerability (CVE-2014-0224)/JSA10629 - Knowledge Bas
mandriva.com

OpenSSL 'ssl3_release_read_buffer()' Use-After-Free Memory Corruption Vulnerability

#2167: openssl-1.0.0-beta5 - fails if used from multiple threads and with SSL_MODE_RELEASE_BUFFERS

Security Advisory SA59342 - HP Smart Update Manager (HP SUM) OpenSSL Multiple Vulnerabilities - Secunia

'[security bulletin] HPSBHF03052 rev.2 - HP Network Products running OpenSSL, Multiple Remote Vulnera' - MARC

FortiGuard.com | Multiple Vulnerabilities in OpenSSL

ViewVC Exception

IBM Security Bulletin: IBM Initiate Master Data Service, IBM InfoSphere Master Data Management are affected by the following OpenSSL vulr

Citrix Security Advisory for OpenSSL Vulnerabilities (June 2014)

Security Advisory SA59655 - IBM SmartCloud Provisioning for IBM Provided Software Virtual Appliance OpenSSL Multiple Vulnerabilities - Se

IBM Security Bulletin: IBM Security Access Manager for Mobile and IBM Security Access Manager for Web appliances are affected by the follo

[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19

Security Advisory SA59287 - IBM Proventia Network Enterprise Scanner OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM InfoSphere Guardium Database Activity Monitor is affected by CVE-2014-0221, CVE-2014-0224, CVE-2014-0195,

VMSA-2014-0012 | United States

Security Advisory SA59437 - IBM Rational Application Developer for WebSphere Software OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: Vulnerabilities in OpenSSL affect IBM SmartCloud Provisioning. - United States

analysis of openssl freelist reuse

Security Advisory SA59666 - IBM SDK for Node.js OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA58713 - IBM Multiple Products OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM Security Proventia Network Enterprise Scanner is affected by the following OpenSSL vulnerabilities: CVE-2014-022

oss-security - Use-after-free race condition,in OpenSSL's read buffer

Security Advisory SA59450 - IBM API Management OpenSSL Multiple Vulnerabilities - Secunia

IBM notice: The page you requested cannot be displayed

Security Bulletin: Rational Application Developer is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-

McAfee KnowledgeBase - McAfee Security Bulletin – Seven OpenSSL vulnerabilities patched in McAfee products

Security Advisory SA59438 - IBM Security Access Manager for Web / Security Access Manager for Mobile Multiple Vulnerabilities - Secunia

'[security bulletin] HPSBMU03057 rev.1 - HP Version Control Agent (HP VCA) running OpenSSL on Linux a' - MARC

'[security bulletin] HPSBMU03056 rev.1 - HP Version Control Repository Manager (HP VCRM) running Open' - MARC

'[security bulletin] HPSBMU03062 rev.1 - HP Insight Control server deployment on Linux and Windows ru' - MARC

Oracle Critical Patch Update - January 2015

IBM Security Bulletin: IBM Security Network Intrusion Prevention System is affected by the following OpenSSL vulnerabilities: CVE-2014-0224

Security Advisory SA59669 - IBM InfoSphere Guardium OpenSSL Security Issue and Multiple Vulnerabilities - Secunia

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

Security Advisory SA59413 - IBM Initiate Master Data Service / IBM InfoSphere Master Data Management OpenSSL Vulnerabilities - Secunia

'[security bulletin] HPSBMU03074 rev.1 - HP Insight Control server migration on Linux and Windows run' - MARC

Security Advisory SA59300 - IBM Tivoli Management Framework OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA59500 - IBM Tivoli Management Framework OpenSSL Multiple Vulnerabilities - Secunia

[security-announce] SUSE-SU-2015:0743-1: important: Security update for

Document Display | HPE Support Center

OpenBSD 5.5 errata

'[security bulletin] HPSBMU03055 rev.1 - HP Smart Update Manager (HP SUM) running OpenSSL, Remote Den' - MARC

IBM Support

#2167: openssl-1.0.0-beta5 - fails if used from multiple threads and with SSL_MODE_RELEASE_BUFFERS

www.novell.com/support/kb/doc.php

Security Advisory SA59490 - HP Version Control Agent OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA58337 - IBM Upward Integration Modules (UIM) OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM® SDK for Node.js™ is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2

Support / Security / Advisories / / MDVSA-2015:062 | Mandriva

Security Advisory SA59721 - IBM SmartCloud Provisioning OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory-Multiple OpenSSL vulnerabilities on Huawei products - Huawei PSIRT

'[security bulletin] HPSBGN03068 rev.1 - HP OneView running OpenSSL, Remote Denial of Service (DoS), ' - MARC

IBM Support

Multiple Vulnerabilities in OpenSSL Affecting Cisco Products

ftp.openbsd.org/pub/OpenBSD/patches/5.5/common/004_openssl.patch.sig

IBM notice: The page you requested cannot be displayed

www.openssl.org/news/secadv_20140605.txt

Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities

Oracle Critical Patch Update - October 2014

Oracle Critical Patch Update - July 2014

Juniper Networks - 2014-06 Out of Cycle Security Bulletin: Vulnerabilities in OpenSSL related to ChangeCipherSpec, DTLS, SSL_MODE_REI

'[security bulletin] HPSBMU03076 rev.2 - HP Systems Insight Manager (SIM) on Linux and Windows runnin' - MARC

IBM Security Bulletin: IBM Sterling Connect:Express for UNIX is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-201

'[security bulletin] HPSBMU03051 rev.2 - HP System Management Homepage running OpenSSL on Linux and W' - MARC

Mageia Advisory: MGASA-2014-0187 - Updated openssl packages fix CVE-2010-5298

IBM Security Bulletin: SmartCloud Orchestrator is affected by the following OpenSSL vulnerabilities (CVE-2014-0224, CVE-2014-0221, CVE-2

IBM notice: The page you requested cannot be displayed

IBM SDK for Node.js 1.1.0.4 for use by the Cordova tools

IBM Security Bulletin: Tivoli Management Framework is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, C

IBM Support

SecurityFocus

www.blackberry.com/btsc/KB36051

IBM Security Bulletin: IBM Security Network Protection is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0198

[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20
Security Advisory SA58939 - IBM SmartCloud Orchestrator OpenSSL Multiple Vulnerabilities - Secunia
IBM Support
VMSA-2014-0006.11 | United States
Security Advisory SA59440 - IBM Security Network Protection Security Issue and Multiple Vulnerabilities - Secunia
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)

590349 Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)