



CVE-2014-0198

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0198
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-06 10:44:00 UTC
Updated	2022-08-29 20:50:00 UTC
Description	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enable

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
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	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	1.0.1g	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	1.0.1g	All	All	All
Application	Openssl	Openssl	All	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	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

[About Secunia Research | Flexera](#)

[CVE-2014-0198 | Puppet Labs](#)

[Bug 1093837 – CVE-2014-0198 openssl: SSL_MODE_RELEASE_BUFFERS NULL pointer dereference in do_ssl3_write\(\)](#)

[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](#)

[Security Advisory SA58945 - IBM FastSetup OpenSSL Multiple Vulnerabilities - Secunia](#)

[Juniper Networks - Junos Pulse/SA \(SSLVPN\): Details on fixes for SSL/TLS MITM vulnerability \(CVE-2014-0224\)/JSA10629 - Knowledge Base](#)

[Mageia Advisory: MGASA-2014-0204 - Updated openssl packages fix CVE-2014-0198](#)

[Security Advisory SA60049 - HP OneView OpenSSL Two Vulnerabilities - Secunia](#)

[OpenSSL 'so_ssl3_write\(\)' Function NULL Pointer Dereference Denial of Service Vulnerability](#)

aix.software.ibm.com/aix/efixes/security/openssl_advisory9.asc

[openSUSE-SU-2014:0635-1: moderate: update for openssl](#)

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
Security Advisory SA59202 - Cisco MATE Multiple Products OpenSSL Two Vulnerabilities - Secunia
Security Advisory SA59514 - HP System Management Homepage OpenSSL Multiple Vulnerabilities - Secunia
FortiGuard.com Multiple Vulnerabilities in OpenSSL
IBM Security Bulletin: IBM Initiate Master Data Service, IBM InfoSphere Master Data Management are affected by the following OpenSSL vuln
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 folk
[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
Security Advisory SA59264 - Cisco WebEx Meetings Server / Unified Communications Manager OpenSSL Multiple Vulnerabilities - Secunia
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
Security Advisory SA59450 - IBM API Management OpenSSL Multiple Vulnerabilities - Secunia
IBM notice: The page you requested cannot be displayed
Security Advisory SA59374 - Cisco IOS XE OpenSSL Multiple Vulnerabilities - Secunia
IBM Security Bulletin: IBM i is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-201
Security Bulletin: Rational Application Developer is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-
Security Advisory SA59282 - Cisco Multiple Products OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA59449 - IBM Security Network Intrusion Prevention System OpenSSL Multiple Vulnerabilities - Secunia
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
About Secunia Research Flexera
'[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
mandriva.com
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

IBM Security Bulletin: IBM Sterling Connect:Express for UNIX is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0222

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

Security Advisory SA58667 - Cisco Multiple Products OpenSSL SSL/TLS Handshake Security Issue and Two Denial of Service Vulnerabilities

Security Advisory SA59310 - Novell Messenger OpenSSL Multiple Vulnerabilities - Secunia

cert-portal.siemens.com/productcert/pdf/ssa-234763.pdf

IBM Security Bulletin: SmartCloud Orchestrator is affected by the following OpenSSL vulnerabilities (CVE-2014-0224, CVE-2014-0221, CVE-2014-0222)

Security Advisory SA59190 - Blue Coat ProxySG OpenSSL SSL/TLS Handshake Security Issue and Denial of Service Vulnerability - Secunia

IBM notice: The page you requested cannot be displayed

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

Security Advisory SA59126 - Huawei Multiple Products Multiple OpenSSL Vulnerabilities - Secunia

Debian -- Security Information -- DSA-2931-1 openssl

IBM Security Bulletin: Tivoli Management Framework is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0222

Security Advisory SA59284 - Cisco Prime Network OpenSSL Multiple Vulnerabilities - Secunia

IBM Support

SecurityFocus

www.blackberry.com/btsc/KB36051

Security Advisory SA61254 - IBM InfoSphere Guardium Database Activity Monitor Multiple Vulnerabilities - Secunia

Security Advisory SA59491 - BlackBerry OS OpenSSL Multiple Vulnerabilities - Secunia

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

Oracle Critical Patch Update - October 2017

IBM Support

support.f5.com/kb/en-us/solutions/public/15000/300/sol15329.html

VMSA-2014-0006.11 | United States

Security Advisory SA59440 - IBM Security Network Protection Security Issue and Multiple Vulnerabilities - Secunia

OpenBSD 5.5 errata

Security Advisory SA59306 - IBM i OpenSSL 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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)