



CVE-2015-0204

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

Summary

CVE	CVE-2015-0204
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-09 02:59:00 UTC
Updated	2018-07-19 01:29:00 UTC
Description	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 contains a buffer overflow that can be exploited to crash the application.

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	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	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	All	All	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	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	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	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All

References

Reference

[security-announce] SUSE-SU-2015:0946-1: important: Security update for

Oracle Bulletin Board Update - January 2015

[security-announce] openSUSE-SU-2015:0130-1: important: Security update

Document Display | HPE Support Center

Oracle Critical Patch Update - July 2016

'[security bulletin] HPSBUX03244 SSRT101885 rev.2 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

[security-announce] SUSE-SU-2015:2182-1: important: Security update for

'[security bulletin] HPSBOV03318 rev.1 - HP SSL for OpenVMS, Remote Denial of Service (DoS) and other' - MARC

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

Red Hat Customer Portal

Oracle Critical Patch Update - October 2015

CVE-2015-0204

Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware

Gentoo Security

Oracle Critical Patch Update - July 2015

OpenSSL CVE-2015-0204 Man in the Middle Security Bypass Vulnerability

'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC

'[security bulletin] HPSBUX03334 SSRT102000 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

Juniper Networks - 2015-04 Security Bulletin: OpenSSL 8th January 2015 advisory.

[security-announce] SUSE-SU-2015:0578-1: important: Security update for

CPU July 2018

'[security bulletin] HPSBUX03162 SSRT101885 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

'[security bulletin] HPSBMU03396 rev.1 - HP Version Control Repository Manager (VCRM) on Windows and ' - MARC

Tracking the FREAK Attack

[security-announce] SUSE-SU-2015:1085-1: important: Security update for

IBM Security Bulletin: Multiple vulnerabilities in IBM Java Runtime affect Tivoli Netcool/OMNibus (Multiple CVEs) - United States

McAfee KnowledgeBase - McAfee Security Bulletin - Firewall Enterprise update fixes 8 OpenSSL CVEs

www.openssl.org/news/secadv_20150319.txt

Red Hat Customer Portal

SA88 : OpenSSL Security Advisory 08-Jan-2015 | Symantec

IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States

McAfee KnowledgeBase - McAfee Security Bulletin - FREAK OpenSSL Vulnerability

[security-announce] SUSE-SU-2015:2192-1: important: Security update for

APPLE-SA-2015-04-08-2 OS X 10.10.3 and Security Update 2015-004

Debian -- Security Information -- DSA-3125-1 openssl
Multiple Vulnerabilities in OpenSSL (January 2015) Affecting Cisco Products
'[security bulletin] HPSBMMU03397 rev.1 - HP Version Control Agent (VCA) on Windows and Linux, Multipl' - MARC
Support / Security / Advisories // MDVSA-2015:062 Mandriva
Support / Security / Advisories // MDVSA-2015:063 Mandriva
[security-announce] SUSE-SU-2015:1161-1: important: Security update for
'[security bulletin] HPSBGN03299 rev.1 - HP IceWall SSO Dfw, SSO Certd, MCRP, and Federation Agent ru' - MARC
SA91 : FREAK Attack Symantec
[security-announce] SUSE-SU-2015:2168-1: important: Security update for
[security-announce] SUSE-SU-2015:1138-1: important: Security update for
Support / Security / Advisories // MDVSA-2015:019 Mandriva
www.openssl.org/news/secadv_20150108.txt
Oracle Critical Patch Update - April 2015
Only allow ephemeral RSA keys in export ciphersuites. · ce325c6 · openssl/openssl · GitHub
[security-announce] SUSE-SU-2015:2216-1: important: Security update for
[security-announce] openSUSE-SU-2016:0640-1: important: Security update
'[security bulletin] HPSBMMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC
Red Hat Customer Portal
HP Version Control Repository Manager Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Condu
'[security bulletin] HPSBMMU03413 rev.1 - HP Virtual Connect Enterprise Manager SDK, Multiple Vulnerab' - MARC
[security-announce] SUSE-SU-2015:2166-1: important: Security update for
IBM X-Force Exchange
Oracle Solaris Third Party Bulletin - April 2015
[security-announce] SUSE-SU-2015:1086-1: important: Security update for
'[security bulletin] HPSBMMU03345 rev.1 - HP Network Node Manager i (NNMi) and Smart Plugins (iSPIs) f' - MARC
'[security bulletin] HPSBHF03289 rev.1- HP ThinClient PCs running ThinPro Linux, Remote Code Executio' - MARC
Oracle Critical Patch Update - October 2017
About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004 - Apple Support
McAfee KnowledgeBase - Intel Security - Security Bulletin: Fourteen OpenSSL CVEs Announced on March 19, 2015
[security-announce] SUSE-SU-2016:0113-1: important: Security update for
Red Hat Customer Portal
Oracle Critical Patch Update - January 2016
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)

[591058](#) Phoenix Contact mGuard devices Vulnerability (Security Advisory 2015/04/07-001)

© [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](#)