



CVE-2015-3197

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

Summary

CVE	CVE-2015-3197
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-15 02:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	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

Risk And Classification

Problem Types: CWE-310 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All

Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	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	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All

Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Application	Oracle	Oss Support Tools	8.11.16.3.8	All	All	All
Application	Oracle	Oss Support Tools	8.11.16.3.8	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.53	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.54	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.53	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.54	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	All	All	All
Application	Oracle	Tuxedo	12.1.1.0	All	All	All
Application	Oracle	Tuxedo	12.1.1.0	All	All	All
Application	Oracle	Vm Virtualbox	5.0.16	All	All	All
Application	Oracle	Vm Virtualbox	5.0.16	All	All	All

References

Reference

Document Display | HPE Support Center

Oracle Critical Patch Update Advisory - April 2016

www.openssl.org/news/secadv/20160128.txt

[security-announce] openSUSE-SU-2016:0637-1: important: Security update

OpenSSL Flaws Let Remote Users Recover DH Keys in Certain Cases and Let Remote Users Negotiate Disabled Ciphers - SecurityTracker

[security-announce] SUSE-SU-2016:0617-1: important: Security update for

Oracle Critical Patch Update - July 2016

[security-announce] openSUSE-SU-2016:0720-1: important: Security update

[security-announce] SUSE-SU-2016:0624-1: important: Security update for

[security-announce] SUSE-SU-2016:0620-1: important: Security update for

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

OpenSSL: Multiple vulnerabilities (GLSA 201601-05) — Gentoo security

FreeBSD-SA-16:11

OpenSSL CVE-2015-3197 Security Bypass Vulnerability

[security-announce] SUSE-SU-2016:1057-1: important: Security update for

Oracle Critical Patch Update - October 2016

[security-announce] openSUSE-SU-2016:0638-1: important: Security update

[security-announce] SUSE-SU-2016:0678-1: important: Security update for

[security-announce] openSUSE-SU-2016:0628-1: important: Security update

[security-announce] SUSE-SU-2016:0631-1: important: Security update for

Vulnerability Note VU#257823 - OpenSSL re-uses unsafe prime numbers in Diffie-Hellman protocol

[security-announce] openSUSE-SU-2016:1241-1: important: Security update

Oracle VM Server for x86 Bulletin - July 2016

[security-announce] SUSE-SU-2016:0641-1: important: Security update for

git.openssl.org Git - openssl.git/commit

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

git.openssl.org Git - openssl.git/commit

Oracle Linux Bulletin - January 2016

Document Display | HPE Support Center

[SECURITY] Fedora 23 Update: openssl-1.0.2f-1.fc23

[security-announce] SUSE-SU-2016:0621-1: important: Security update for

Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates

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

[security-announce] openSUSE-SU-2016:1239-1: important: Security update

Oracle Critical Patch Update - July 2017

Oracle Critical Patch Update - October 2017

Oracle Solaris Bulletin - 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)

0011)

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

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

[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](#)