



CVE-2014-3510

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-3510
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-13 23:55:00 UTC
Updated	2023-11-07 02:20:00 UTC
Description	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1o has a buffer overflow in the SSL3_SEND_CLIENT_KEY_EXCHANGE function. A remote attacker can exploit this to cause a denial of service or possibly execute arbitrary code.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	0.9.8za	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	1.0.0m	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	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	beta 1	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	0.9.8za	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	1.0.0m	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

References

Reference

'[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC

git.openssl.org Git - [openssl.git/commit](https://git.openssl.org/commit)

Security Advisory SA60687 - Red Hat update for openssl - Secunia
Red Hat Customer Portal
www.openssl.org/news/secadv_20140806.txt
About Secunia Research Flexera
git.openssl.org Git - openssl.git/commit
'[security bulletin] HPSBOV03099 rev.1 - HP OpenVMS running OpenSSL, Remote Denial of Service (DoS) o' - MARC
About Secunia Research Flexera
Security Bulletin: Multiple Vulnerabilities in Current Release of IBM® SDK for Node.js™
Security Advisory-9 OpenSSL Vulnerabilities on Huawei products - Huawei PSIRT
[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19
'[security bulletin] HPSBUX03095 SSRT101674 rev.1 - HP-UX running OpenSSL, Multiple Vulnerabilities' - MARC
Security Advisory SA61184 - IBM SDK for Node.js Multiple Vulnerabilities - Secunia
About Secunia Research Flexera
IBM Security Bulletin: - United States
Security Advisory SA61100 - syslog-ng Premium Edition OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA60221 - SUSE update for openssl - Secunia
About Secunia Research Flexera
OpenSSL Bugs Let Remote Users Deny Service, Obtain Information, and Potentially Execute Arbitrary Code - SecurityTracker
www.mandriva.com
NetBSD-SA2014-008
OpenSSL: Multiple vulnerabilities (GLSA 201412-39) — Gentoo Security
Security Advisory SA61775 - Huawei Multiple Products Multiple OpenSSL Vulnerabilities - Secunia
Debian -- Security Information -- DSA-2998-1 openssl
About Secunia Research Flexera
SOL15568 - OpenSSL vulnerability CVE-2014-3510
Security Advisory SA61250 - HP OpenVMS update for SSL - Secunia
Red Hat Customer Portal
linux.oracle.com ELSA-2014-1052
About Secunia Research Flexera
IBM notice: The page you requested cannot be displayed
Security Advisory SA59743 - OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA60778 - HP-UX update for OpenSSL - Secunia
IBM X-Force Exchange
About Secunia Research Flexera
FreeBSD-SA-14:18
'[security bulletin] HPSBUX03095 SSRT101674 rev.1 - HP-UX running OpenSSL, Multiple Vulnerabilities' - MARC

[syslog-ng-announce] syslog-ng Premium Edition 5 LTS (5.0.0a) has been released

Security Advisory SA61959 - IBM Tivoli Management Framework Multiple Vulnerabilities - Secunia

1127503 – (CVE-2014-3510) CVE-2014-3510 openssl: DTLS anonymous (EC)DH denial of service

About Secunia Research | Flexera

Security Advisory SA60493 - IBM i OpenSSL Multiple Vulnerabilities - Secunia

About Secunia Research | Flexera

About Secunia Research | Flexera

IBM Security Bulletin: Multiple vulnerabilities in OpenSSL affect IBM Tivoli Composite Application Manager for Transactions (CVE-2014-3508,

Security Advisory SA60938 - NetBSD update for openssl - Secunia

About Secunia Research | Flexera

Security Advisory SA60803 - SUSE update for openssl1 - Secunia

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

aix.software.ibm.com/aix/efixes/security/openssl_advisory10.asc

openSUSE-SU-2014:1052-1: moderate: update for openssl

[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20

Security Advisory SA59221 - Oracle Linux update for openssl - Secunia

OpenSSL DTLS CVE-2014-3510 Remote Denial of Service Vulnerability

linux.oracle.com | ELSA-2014-1053 - openssl security update

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)

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

[671109](#) EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2509)

© 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