



CVE-2014-3512

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2014-3512 |
| 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 | Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote att |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-------------------------|-------------------------|---------|--------|---------|----------|
| 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 | 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

support.f5.com/kb/en-us/solutions/public/15000/500/sol15565.html

www.openssl.org/news/secadv_20140806.txt

About Secunia Research | Flexera

About Secunia Research | Flexera

OpenSSL SRP CVE-2014-3512 Remote Denial of Service Vulnerability

Security Bulletin: Multiple Vulnerabilities in Current Release of IBM® SDK for Node.js™

Security Advisory-9 OpenSSL Vulnerabilities on Huawei products - Huawei PSIRT

Security Advisory SA61184 - IBM SDK for Node.js Multiple Vulnerabilities - Secunia

IBM Security Bulletin: - United States

Security Advisory SA61100 - syslog-ng Premium Edition OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA60221 - SUSE update for openssl - Secunia

[R2] OpenSSL Protocol Downgrade Vulnerability Affects Tenable Products | Tenable Network Security

OpenSSL Bugs Let Remote Users Deny Service, Obtain Information, and Potentially Execute Arbitrary Code - SecurityTracker

Security Advisory SA61171 - F5 LineRate Multiple OpenSSL Vulnerabilities - Secunia

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

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

IBM notice: The page you requested cannot be displayed

| |
|--|
| About Secunia Research Flexera |
| FreeBSD-SA-14:18 |
| [syslog-ng-announce] syslog-ng Premium Edition 5 LTS (5.0.6a) has been released |
| Security Advisory SA61959 - IBM Tivoli Management Framework Multiple Vulnerabilities - Secunia |
| 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, |
| About Secunia Research Flexera |
| Security Advisory SA60803 - SUSE update for openssl1 - Secunia |
| IBM X-Force Exchange |
| aix.software.ibm.com/aix/efixes/security/openssl_advisory10.asc |
| openSUSE-SU-2014:1052-1: moderate: update for openssl |
| Security Advisory SA60810 - Tenable SecurityCenter Multiple OpenSSL Vulnerabilities - Secunia |
| CVE Program record |
| NVD vulnerability detail |
|  |
| No vendor comments have been submitted for this CVE. |
| Legacy QID Mappings |
| 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](#)