



# CVE-2014-3511

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

## Summary

<b>CVE</b>	CVE-2014-3511
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-08-13 23:55:00 UTC
<b>Updated</b>	2023-11-07 02:20:00 UTC
<b>Description</b>	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to forc

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta4	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta5	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	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	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1h	All	All	All

## References

### Reference

About Secunia Research | Flexera

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

'[security bulletin] HPSBMU03267 rev.1 - HP Matrix Operating Environment and HP CloudSystem Matrix ru' - MARC

'[security bulletin] HPSBMU03263 rev.3 - HP Insight Control running OpenSSL, Remote Disclosure of Inf' - MARC

[www.openssl.org/news/secadv\\_20140806.txt](http://www.openssl.org/news/secadv_20140806.txt)

About Secunia Research | Flexera

IBM X-Force Exchange

About Secunia Research | Flexera

'[security bulletin] HPSBMU03216 rev.2 - HP Service Manager running SSLv3, Multiple Remote Vulnerabil' - MARC

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

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

Red Hat Customer Portal

[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19

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

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

Red Hat Customer Portal

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

SOL15564 - TLS vulnerability CVE-2014-3511

Security Advisory SA59887 - Tenable Appliance OpenSSL Vulnerability - Secunia

Splunk Enterprise 6.1.4 and 5.0.10 address four vulnerabilities | Splunk

Document Display   HPE Support Center
OpenSSL Bugs Let Remote Users Deny Service, Obtain Information, and Potentially Execute Arbitrary Code - SecurityTracker
Security Advisory SA60377 - Aruba Multiple Products OpenSSL TLS Downgrade Security Bypass Vulnerability - Secunia
1127504 – (CVE-2014-3511) CVE-2014-3511 openssl: TLS protocol downgrade attack
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
McAfee KnowledgeBase - McAfee Security Bulletin - ePO update fixes a security vulnerability reported by OpenSSL
Security Advisory SA60890 - McAfee ePolicy Orchestrator Java and OpenSSL Multiple Vulnerabilities - Secunia
Nothing found for Support Alerts Aid 08182014 Txt
OpenSSL Vulnerabilities related to Version 1.0.1i   Techzone
linux.oracle.com   ELSA-2014-1052
git.openssl.org Git - openssl.git/commit
About Secunia Research   Flexera
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
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 SA61043 - F5 Multiple Products OpenSSL ClientHello Ciphersuite Downgrade Vulnerability - Secunia
'[security bulletin] HPSBMU03304 rev.1 - HP Insight Control server deployment on Linux and Windows, R' - MARC
Security Advisory SA60803 - SUSE update for openssl1 - Secunia
aix.software.ibm.com/aix/efixes/security/openssl_advisory10.asc
openSUSE-SU-2014:1052-1: moderate: update for openssl
OpenSSL CVE-2014-3511 Man in the Middle Security Bypass Vulnerability
Document Display   HPE Support Center

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

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

'[security bulletin] HPSBMU03260 rev.1 - HP System Management Homepage running OpenSSL on Linux and W' - MARC

'[security bulletin] HPSBMU03261 rev.2 - HP Systems Insight Manager running OpenSSL on Linux and Wind' - MARC

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

[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)

© [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](#)**