



# CVE-2014-3572

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

## Summary

<b>CVE</b>	CVE-2014-3572
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-01-09 02:59:00 UTC
<b>Updated</b>	2017-11-15 02:29:00 UTC
<b>Description</b>	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

## Risk And Classification

### Problem Types: CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0a	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	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0n	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0o	All	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	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

Oracle Critical Patch Update - July 2016

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

Oracle Critical Patch Update - October 2015

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

Oracle Critical Patch Update - July 2015

'[security bulletin] HPSBGN03299 rev.1 - HP IceWall SSO Dfw, SSO Certd, MCRP, and Federation Agent ru' - MARC

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

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

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

'[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

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

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

McAfee KnowledgeBase - McAfee Security Bulletin - FREAK OpenSSL Vulnerability

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

'[security bulletin] HPSBMU03397 rev.1 - HP Version Control Agent (VCA) on Windows and Linux, Multipl' - MARC

ECDH downgrade bug fix. · b15f876 · openssl/openssl · GitHub

Support / Security / Advisories // MDVSA-2015:062 | Mandriva

Support / Security / Advisories // MDVSA-2015:019 | Mandriva

[www.openssl.org/news/secadv\\_20150108.txt](http://www.openssl.org/news/secadv_20150108.txt)

Oracle Critical Patch Update - April 2015

[security-announce] openSUSE-SU-2015:1277-1: important: Security update

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

'[security bulletin] HPSBMU03380 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] HPSBMU03413 rev.1 - HP Virtual Connect Enterprise Manager SDK, Multiple Vulnerab' - MARC

'[security bulletin] HPSBHF03289 rev.1- HP ThinClient PCs running ThinPro Linux, Remote Code Executio' - MARC

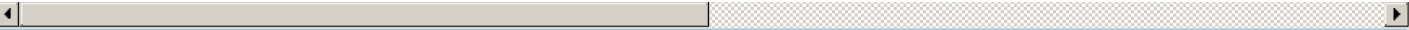
Oracle Critical Patch Update - October 2017

About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004 - Apple Support

OpenSSL CVE-2014-3572 Security Bypass Vulnerability

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)

© [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](#)