



CVE-2013-4353

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

Summary

CVE	CVE-2013-4353
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-09 01:55:00 UTC
Updated	2023-11-07 02:16:00 UTC
Description	The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service.

Risk And Classification

Problem Types: CWE-20

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	1.0.1	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
-------------	-------------------------	-------------------------	--------	-----	-----	-----

References

Reference

- Debian -- Security Information -- DSA-2837-1 openssl
- git.openssl.org/gitweb
- [git.openssl.org Git - openssl.git/commit](https://git.openssl.org/Git)
- USN-2079-1: OpenSSL vulnerabilities | Ubuntu
- openSUSE-SU-2014:0096-1: moderate: update for openssl
- openSUSE-SU-2014:0099-1: moderate: update for openssl
- [SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19
- Red Hat Customer Portal
- Bug 1049058 – CVE-2013-4353 openssl: client NULL dereference crash on malformed handshake packets
- IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.3.0.1 Interim Fix 29 README Tivoli Composite Appl
- [git.openssl.org Git](https://git.openssl.org/Git)
- IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.4 Interim Fix 13 README Tivoli Composite Applicat
- OpenSSL: OpenSSL vulnerabilities
- [git.openssl.org Git - openssl.git/commit](https://git.openssl.org/Git)
- openSUSE-SU-2014:0094-1: moderate: update for openssl
- [SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20
- Red Hat Customer Portal
- Splunk 6.0.3 addresses two vulnerabilities - April 10, 2014 | Splunk
- 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)

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](#)