



# CVE-2016-6302

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

## Summary

<b>CVE</b>	CVE-2016-6302
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-09-16 05:59:00 UTC
<b>Updated</b>	2023-11-07 02:33:00 UTC
<b>Description</b>	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation o

## 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	1.0.1a	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
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All

Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.1s	All	All	All
Application	Openssl	Openssl	1.0.1t	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2g	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.1	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
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.1s	All	All	All
Application	Openssl	Openssl	1.0.1t	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2h	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	6	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	6	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.3	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.3	All	All	All

## References

### Reference

[/news/vulnerabilities.html](#)

[Oracle Critical Patch Update - January 2018](#)

[Oracle Critical Patch Update - April 2018](#)

[Splunk Enterprise 6.4.5 addresses multiple vulnerabilities | Splunk](#)

[Oracle Linux Bulletin - October 2016](#)

[Oracle Critical Patch Update - October 2016](#)

[Public KB - SA40312 - September 22 2016 OpenSSL Security Advisory](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[OpenSSL CVE-2016-6302 Denial of Service Vulnerability](#)

[\[R5\] Nessus 6.9 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security](#)

[SA132 : OpenSSL Vulnerabilities 22-Sep-2016 and 26-Sep-2016](#)

[OpenSSL Multiple Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker](#)

[cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf](#)

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

[Splunk Enterprise 6.5.1 addresses multiple OpenSSL vulnerabilities | Splunk](#)

[Red Hat Customer Portal](#)

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

Oracle VM Server for x86 Bulletin - October 2016

[R2] PVS 5.2.0 Fixes Multiple Third-party Library Vulnerabilities - Security Advisory | Tenable Network Security

Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates

Red Hat Customer Portal

IBM Security Bulletin: Vulnerabilities in OpenSSL, OpenVPN and GNU glibc affect IBM Security Virtual Server Protection for VMware - United

Oracle Solaris Bulletin - October 2016

Oracle Critical Patch Update - July 2017

[R1] LCE 4.8.2 Fixes Multiple Third-party Library Vulnerabilities - Security Advisory | Tenable Network Security

Oracle Critical Patch Update - October 2017

FreeBSD-SA-16:26

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)

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

© [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](#)