CVE-2016-2181

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-2181
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-16 05:59:00 UTC
Updated	2023-11-07 02:31:00 UTC
Description	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch numbe

Risk And Classification

Problem Types: CWE-189

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	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
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All

References

Reference
[security-announce] openSUSE-SU-2016:2537-1: important: Security update for compat-openssl098 - openSUSE Security Announce - openS
[security-announce] SUSE-SU-2016:2394-1: important: Security update for
OpenSSL CVE-2016-2181 Denial of Service Vulnerability
[security-announce] SUSE-SU-2016:2458-1: important: Security update for
[security-announce] SUSE-SU-2016:2468-1: important: Security update for
/news/vulnerabilities.html
Oracle Critical Patch Update - January 2018
Oracle Critical Patch Update - April 2018
USN-3087-1: OpenSSL vulnerabilities | Ubuntu
Splunk Enterprise 6.4.5 addresses multiple vulnerabilities | Splunk
Oracle Linux Bulletin - October 2016
Oracle Critical Patch Update - October 2016
[security-announce] openSUSE-SU-2018:0458-1: important: Security update
git.openssl.org Git - openssl.git/commit
Debian -- Security Information -- DSA-3673-1 openssl
Public KB - SA40312 - September 22 2016 OpenSSL Security Advisory
[security-announce] openSUSE-SU-2016:2407-1: important: Security update
[security-announce] SUSE-SU-2016:2469-1: important: Security update for
OpenSSL DTLS Replace Protection Sequence Number Processing Errors Let Remote Users Deny Service - SecurityTracker
[security-announce] openSUSE-SU-2016:2391-1: important: Security update
Knowledge Center

Security Advisory 0024 - Arista
Red Hat Customer Portal
[R5] Nessus 6.9 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security
[security-announce] SUSE-SU-2017:2700-1: important: Security update for SLES 12-SP1 Docker image - openSUSE Security Announce - ope
USN-3087-2: OpenSSL regression | Ubuntu
SA132 : OpenSSL Vulnerabilities 22-Sep-2016 and 26-Sep-2016
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf
Splunk Enterprise 6.5.1 addresses multiple OpenSSL vulnerabilities | Splunk
Oracle VM Server for x86 Bulletin - October 2016
git.openssl.org Git - openssl.git/commit
[R2] PVS 5.2.0 Fixes Multiple Third-party Library Vulnerabilities - Security Advisory | Tenable Network Security
Full Disclosure: Orion Elite Hidden IP Browser Pro - All Versions - Multiple Known Vulnerabilities
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates
[security-announce] SUSE-SU-2017:2699-1: important: Security update for
Security Advisory - Sixteen OpenSSL Vulnerabilities on Some Huawei products
[security-announce] SUSE-SU-2016:2387-1: important: Security update for
IBM Security Bulletin: Vulnerabilities in OpenSSL, OpenVPN and GNU glibc affect IBM Security Virtual Server Protection for VMware - United
support.f5.com/csp/article/K59298921
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)

671073 EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2643)

671109 EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2509)

© 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 registred 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