CVE-2016-6309

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-6309
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-26 19:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote at

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.282120000 probability, percentile 0.965230000 (date 2026-05-07)

Problem Types: CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.1.0a	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Document Display | HPE Support Center
Oracle Critical Patch Update - October 2016
SA132 : OpenSSL Vulnerabilities 22-Sep-2016 and 26-Sep-2016
www.openssl.org/news/secadv/20160926.txt
git.openssl.org Git - openssl.git/commit
OpenSSL Multiple Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker
OpenSSL CVE-2016-6309 Remote Code Execution Vulnerability
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates
Oracle Critical Patch Update - January 2018

Oracle Critical Patch Update - January 2018
Oracle Critical Patch Update - April 2018
IBM Security Bulletin: Vulnerabilities in OpenSSL, OpenVPN and GNU glibc affect IBM Security Virtual Server Protection for VMware - United
Oracle Critical Patch Update - July 2017
[R2] PVS 5.2.0 Fixes Multiple Third-party Library Vulnerabilities - Security Advisory | Tenable Network Security
[R5] Nessus 6.9 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security
git.openssl.org Git - openssl.git/commit
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**