



CVE-2016-1978

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

Summary

CVE	CVE-2016-1978
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-13 18:59:27 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NS

Risk And Classification

Primary CVSS: v3.0 7.3 HIGH from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

Vendor Declared Affected Products

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

References

Reference

1209546 – (CVE-2016-1978) Potential UAF in ssl3_HandleECDHServerKeyExchange

[security-announce] SUSE-SU-2016:0909-1: important: Security update for

[security-announce] SUSE-SU-2016:0727-1: important: Security update for

Red Hat Customer Portal

NSS 3.21 release notes - Mozilla | MDN

USN-2973-1: Thunderbird vulnerabilities | Ubuntu

Debian -- Security Information -- DSA-3688-1 nss

Oracle VM Server for x86 Bulletin - July 2016

Network Security Services (NSS) SSL DHE/ECDHE Use-After-Free Memory Error May Let Remote Users Execute Arbitrary Code on the Targ

Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security
Mozilla Network Security Services Use After Free CVE-2016-1978 Remote Code Execution Vulnerability
Oracle Critical Patch Update - July 2016
Use-after-free in NSS during SSL connections in low memory — Mozilla
[security-announce] SUSE-SU-2016:0820-1: important: Security update for
[security-announce] SUSE-SU-2016:0777-1: important: Security update for
Broadcom Support Portal
Oracle Linux Bulletin - April 2016
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities
Red Hat Customer Portal
Red Hat Customer Portal
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.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)