



CVE-2019-11727

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-11727
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-23 14:15:00 UTC
Updated	2019-07-30 23:15:00 UTC
Description	A vulnerability exists where it possible to force Network Security Services (NSS) to sign CertificateVerify with PKCS#1 v1.5

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

References

Reference	Source	Link	Tags
Security vulnerabilities fixed in Firefox 68 — Mozilla	MISC	www.mozilla.org	Vendor Advisory
Mozilla Firefox: Multiple vulnerabilities (GLSA 201908-12) — Gentoo security	GENTOO	security.gentoo.org	
[security-announce] openSUSE-SU-2019:2251-1: important: Security update	SUSE	lists.opensuse.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Access Denied	MISC	bugzilla.mozilla.org	Issue Tracking, Permissio
[security-announce] openSUSE-SU-2019:2249-1: important: Security update	SUSE	lists.opensuse.org	
[security-announce] openSUSE-SU-2020:0008-1: moderate: Security update f	SUSE	lists.opensuse.org	
[security-announce] openSUSE-SU-2019:2260-1: important: Security update	SUSE	lists.opensuse.org	
[security-announce] openSUSE-SU-2019:2248-1: important: Security update	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296080](#) Oracle Solaris 11.4 Support Repository Update (SRU) 13.4.0 Missing (CPUJUL2019)

[352469](#) Amazon Linux Security Advisory for nspr, nss-softokn, nss-util: ALAS-2021-1522

[377524](#) Alibaba Cloud Linux Security Update for nss and nspr (ALINUX2-SA-2020:0173)

[710148](#) Gentoo Linux Mozilla Firefox Multiple vulnerabilities (GLSA 201908-12)

© [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](#)