



# CVE-2019-11719

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-11719
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-23 14:15:00 UTC
<b>Updated</b>	2020-09-30 18:15:00 UTC
<b>Description</b>	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bou

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Thunderbird</a>	All	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Thunderbird</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Security vulnerabilities fixed in Firefox 68 — Mozilla	MISC	<a href="http://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
[security-announce] openSUSE-SU-2019:1990-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Mozilla Firefox: Multiple vulnerabilities (GLSA 201908-12) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
[security-announce] openSUSE-SU-2019:1813-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	
[SECURITY] [DLA 2388-1] nss security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
Access Denied	MISC	<a href="http://bugzilla.mozilla.org">bugzilla.mozilla.org</a>	Issue Tracking, Permi
[security-announce] openSUSE-SU-2019:1811-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	

[security-announce] openSUSE-SU-2019:2249-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Security vulnerabilities fixed in Firefox ESR 60.8 — Mozilla	MISC	<a href="https://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
Security vulnerabilities fixed in Thunderbird 60.8 — Mozilla	MISC	<a href="https://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 201908-20) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
[security-announce] openSUSE-SU-2019:2248-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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)
- [296081](#) Oracle Solaris 11.4 Support Repository Update (SRU) 12.5.0 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)
- [500919](#) Alpine Linux Security Update for firefox-esr
- [504784](#) Alpine Linux Security Update for firefox-esr
- [710140](#) Gentoo Linux Mozilla Thunderbird Multiple vulnerabilities (GLSA 201908-20)
- [710148](#) Gentoo Linux Mozilla Firefox Multiple vulnerabilities (GLSA 201908-12)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)