CVE-2019-11719

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: CWE-125

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
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References

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

[security-announce] openSUSE-SU-2019:2249-1: important: Security update	SUSE	lists.opensuse.org	
Security vulnerabilities fixed in Firefox ESR 60.8 — Mozilla	MISC	www.mozilla.org	Vendor Advisory
Security vulnerabilities fixed in Thunderbird 60.8 — Mozilla	MISC	www.mozilla.org	Vendor Advisory
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 201908-20) — Gentoo security	GENTOO	security.gentoo.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)
- 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)