CVE-2019-17023

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-17023
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-08 22:15:00 UTC
Updated	2023-01-27 18:24:00 UTC
Description	After a HelloRetryRequest has been sent, the client may negotiate a lower protocol that TLS 1.3, resulting in an invalid state

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

References

Reference	Source	Link	Tags
USN-4234-1: Firefox vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advisory
Access Denied	MISC	bugzilla.mozilla.org	Permissions Required

Debian -- Security Information -- DSA-4726-1 nss	DEBIAN	www.debian.org	
USN-4397-1: NSS vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Security Vulnerabilities fixed in Firefox 72 — Mozilla	CONFIRM	www.mozilla.org	Vendor Advisory
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

- 296071 Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)
- 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)
- 500456 Alpine Linux Security Update for nss
- 500945 Alpine Linux Security Update for firefox
- 503830 Alpine Linux Security Update for firefox
- 940400 AlmaLinux Security Update for nss and nspr (ALSA-2020:3280)
- 960710 Rocky Linux Security Update for nss and nspr (RLSA-2020:3280)