



# CVE-2019-17023

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-17023
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-08 22:15:00 UTC
<b>Updated</b>	2023-01-27 18:24:00 UTC
<b>Description</b>	After a HelloRetryRequest has been sent, the client may negotiate a lower protocol than 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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
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

## References

Reference	Source	Link	Tags
USN-4234-1: Firefox vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>	Third Party Advisory
Access Denied	MISC	<a href="#">bugzilla.mozilla.org</a>	Permissions Required

Debian -- Security Information -- DSA-4726-1 nss	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
USN-4397-1: NSS vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>	
Security Vulnerabilities fixed in Firefox 72 — Mozilla	CONFIRM	<a href="http://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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)

© [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](#)