



CVE-2020-15679

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

Summary

CVE	CVE-2020-15679
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-22 20:15:00 UTC
Updated	2022-12-29 19:16:00 UTC
Description	An OAuth session fixation vulnerability existed in the VPN login flow, where an attacker could craft a custom login URL, cor

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
New non-polling authentication flow. · mozilla-mobile/guardian-vpn-android@981c840 · GitHub	MISC	github.com
PGAND-410 Resolve oauth session fixation on iOS (#272) · mozilla-mobile/guardian-vpn-ios@4309f5c · GitHub	MISC	github.com
New non-polling authentication flow. · mozilla-services/guardian-vpn-windows-deprecated@ac6f562 · GitHub	MISC	github.com
OAuth session fixation vulnerability in Mozilla VPN — Mozilla	MISC	www.mozilla.o
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)