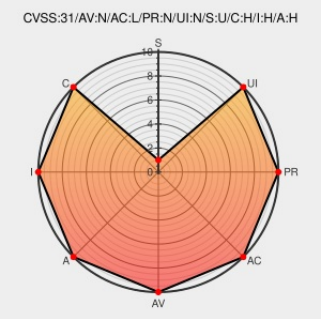
CVE-2021-29978

Published on: 08/05/2021 12:00:00 AM UTC

Last Modified on: 08/13/2021 01:12:00 PM UTC

CVE-2021-29978

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mozilla Vpn from Mozilla contain the following vulnerability:

Multiple low security issues were discovered and fixed in a security audit of Mozilla VPN 2.x branch as part of a 3rd party security audit. This vulnerability affects Mozilla VPN < 2.3.

CVE-2021-29978 has been assigned by security@mozilla.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Mozilla** - **Mozilla VPN** version **< 2.3**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
FVP-02-003 General: Balrog incorrectly verifies certificate chain · Issue #798 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/798

FVP-02-005 WP1-3: Authenticationlistener allows disturbance of login · Issue #800 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/800
FVP-02-002 WP1: Balrog does not verify certificate chain on macOS · Issue #797 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/797
FVP-02-012 WP5: Unencrypted shared preferences · Issue #808 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/808
FVP-02-010 WP5: Android app supports insecure v1 signature · Issue #805 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/805
FVP-02-008 WP5: Android app allows backups of application data · Issue #803 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/803
FVP-02-014 General: Cross-site WebSocket hijacking · Issue #810 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/810
FVP-02-009 WP5: Secure flag missing on views for Android app · Issue #804 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/804
Multiple Low Security Issues in Mozilla VPN — Mozilla	www.mozilla.org text/html	MISC www.mozilla.org/security/advisories/mfsa2021-31/
FVP-02-006 WP3: Race condition in Ping Sender could expose gateway IP · Issue #801 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/801
FVP-02-013 WP5: Android app exposes sensitive data to system logs · Issue #809 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/809
FVP-02-005 WP1-3: Authenticationlistener allows disturbance of login by bakulf · Pull Request #816 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/pull/816
FVP-02-016 OAuth: Auth code could be leaked by injecting port · Issue #812 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/812
FVP-02-011 API: Information disclosure via device endpoint · Issue #806 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/806
FVP-02-004 WP4: ATS policy unnecessarily weakened · Issue #799 · mozilla-mobile/mozilla-vpn-client · GitHub	github.com text/html	MISC github.com/mozilla-mobile/mozilla-vpn-client/issues/799

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:mozilla:mozilla_vpn:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29978 : Multiple low security issues were discovered and fixed in a security audit of Mozilla VPN 2.x bran… twitter.com/i/web/status/1…	2021-08-05 20:16:16

← Previous ID

Next ID→