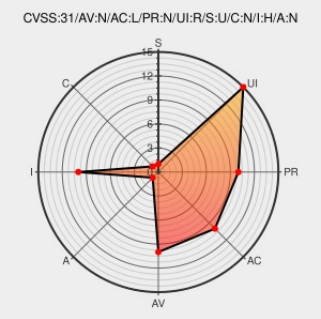
CVE-2020-12414

Published on: 07/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:36 PM UTC

CVE-2020-12414

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

IndexedDB should be cleared when leaving private browsing mode and it is not, the API for WKWebViewConfiguration was being used incorrectly and requires the private instance of this object be deleted when leaving private mode. This vulnerability affects Firefox for iOS < 27.

CVE-2020-12414 has been assigned by security@mozilla.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mozilla** - **Firefox for iOS** version **< 27**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Vulnerabilities fixed in Firefox for iOS 27 —	Vendor Advisory	MISC www.mozilla.org/security/advisories/mfsa2020-

Mozilla	www.mozilla.org text/html	23/
Access Denied	Issue Tracking Permissions Required Vendor Advisory bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=1646756

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:iphone_os:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:iphone_os:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→