



CVE-2020-12413

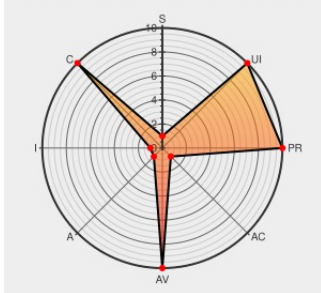
Published on: Not Yet Published

Last Modified on: 02/28/2023 07:49:00 PM UTC

CVE-2020-12413

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Firefox](#) from [Mozilla](#) contain the following vulnerability:

The Raccoon attack is a timing attack on DHE ciphersuites inherit in the TLS specification. To mitigate this vulnerability, Firefox disabled support for DHE ciphersuites.

CVE-2020-12413 has been assigned by [m](#) security@mozilla.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox** version < 78

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox ESR** version < 68.10

CVSS3 Score: **5.9 - MEDIUM**

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

CVE References

Description	Tags	Link
Raccoon Attack	raccoon-attack.com text/html	MISC raccoon-attack.com/
1641795 - (CVE-2020-12413) Raccoon Attack (TLS specification timing side-channel)	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=CVE-2020-12413

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

Related QID Numbers

180667 Debian Security Update for nss (CVE-2020-12413)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox ESR	All	All	All	All
cpe:2.3:a:mozilla:firefox:*.*.*.*.*.*.*.*:						
cpe:2.3:a:mozilla:firefox_esr:*.*.*.*.*.*.*.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @management_sun	IT Risk:F5 Networks.F5OS,Traffix SDCrに脆弱性 Network Appliance CVE-2020-12413 support.f5.com/csp/article/K2... auscert.org.au/bulletins/ESB-...	2021-09-15 05:10:27

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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