



CVE-2022-4066

Published on: Not Yet Published

Last Modified on: 11/28/2022 01:41:00 PM UTC

CVE-2022-4066

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

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



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

A vulnerability was found in davidmoreno onion. It has been rated as problematic. Affected by this issue is the function `onion_response_flush` of the file `src/onion/response.c` of the component Log Handler. The manipulation leads to allocation of resources. The name of the patch is

`de8ea938342b36c28024fd8393ebc27b8442a161`. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-214028.

CVE-2022-4066 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [davidmoreno](#) - **onion** version **n/a**

CVSS3 Score: **8.2 - HIGH**

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

CVE References

Description	Tags	Link
CVE-2022-4066 davidmoreno onion Log response.c onion_response_flush allocation of resources (ID 308)	vuldb.com text/html	MISC vuldb.com/?id.214028
Fix a potential log spamming and DOS attack by kulkom · Pull Request #308 · davidmoreno/onion · GitHub	github.com text/html	MISC github.com/davidmoreno/onion/pull/308

Merge pull request #308 from
kulkom/master ·
davidmoreno/onion@de8ea93 ·
GitHub

[github.com](#)
[text/html](#)

 MISC
github.com/davidmoreno/onion/commit/de8ea938342b36c28024fd8393ebc27b8442a161

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	-	All	All	All
Application	Onion Project	Onion	All	All	All	All
cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:						
cpe:2.3:a:onion_project:onion:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @PentestingN	CVE-2022-40664: Apache Shiro Authentication Bypass Flaw securityonline.info/cve-2022-40664... Penetration Testing CVE-2022-4066... twitter.com/i/web/status/1...	2022-10-12 12:14:08
 /r/netcve	CVE-2022-4066	2022-11-19 20:38:07

[← 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](#)