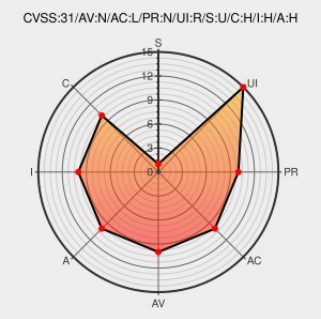
CVE-2020-24772

Published on: Not Yet Published

Last Modified on: 03/29/2022 01:57:00 PM UTC

CVE-2020-24772

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



Certain versions of Clash from Clash Project contain the following vulnerability:

In Dreamacro Clash for Windows v0.11.4, an attacker could embed a malicious iframe in a website with a crafted URL that would launch the Clash Windows client and force it to open a remote SMB share. Windows will perform NTLM authentication when opening the SMB share and that request can be relayed (using a tool like responder) for code execution (or captured for hash cracking).

CVE-2020-24772 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
[Clash for Windows] URL Scheme security issue · Issue #910 · Dreamacro/clash · GitHub	github.com text/html	MISC github.com/Dreamacro/clash/issues/910

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clash Project	Clash	0.11.4	All	All	All

cpe:2.3:a:clash_project:clash:0.11.4:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-24772 : In Dreamacro 1.1.0, an attacker could embed a malicious iframe in a website with a crafted URL tha… twitter.com/i/web/status/1…	2022-03-21 15:05:00
@Festering_Ruin	New vulnerability on the NVD: CVE-2020-24772 March 21, 2022 at 08:15AM ift.tt/DBOkfac	2022-03-21 16:12:19
/r/netcve	CVE-2020-24772	2022-03-21 16:38:17

← 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 registred 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