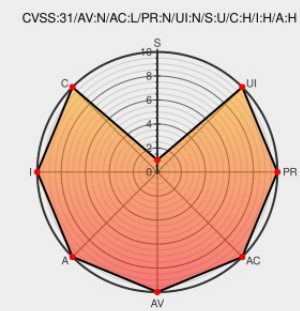
CVE-2023-24205

Published on: Not Yet Published

Last Modified on: 03/03/2023 04:50:00 PM UTC

CVE-2023-24205

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



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

Clash for Windows v0.20.12 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via overwriting the configuration file (cfw-setting.yaml).

CVE-2023-24205 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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

CVE References

Description	Tags	Link
GitHub - Fndroid/clash_for_windows_pkg: A Windows/macOS GUI based on Clash	github.com text/html	MISC github.com/Fndroid/clash_for_windows_pkg
[Bug]: Remote Code Execution/远程代码执行 · Issue #3891 · Fndroid/clash_for_windows_pkg · GitHub	github.com text/html	MISC github.com/Fndroid/clash_for_windows_pkg/issues/3891

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	0.20.12	All	All	All

cpe:2.3:a:clash_project:clash:0.20.12:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-24205 : Clash for #Windows v0.20.12 was discovered to contain a remote code execution RCE vulnerability… twitter.com/i/web/status/1…	2023-02-23 22:09:16
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-24205 Clash for Windows v0.20.12 was discovered to contain a remote cod… twitter.com/i/web/status/1…	2023-02-23 22:55:58
/r/netcve	CVE-2023-24205	2023-02-23 22:38:33

← Previous ID

Next ID→