



CVE-2022-31854

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-31854
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-07 13:15:00 UTC
Updated	2022-10-28 19:27:00 UTC
Description	Codoforum v5.1 was discovered to contain an arbitrary file upload vulnerability via the logo change option in the admin panel.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codologic	Codoforum	5.1	All	All	All

References

Reference	Source	Link	Tags
CODOFORUM - Free PHP Forum Software Script	MISC	codoforum.com	
CodoForum 5.1 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE-2022-31854/exploit.py at main · Vikaran101/CVE-2022-31854 · GitHub	MISC	github.com	
CodoForum V5.1 authenticated RCE My first CVE - Vikaran - Medium	MISC	vikaran101.medium.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report