



CVE-2021-42171

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

Summary

CVE	CVE-2021-42171
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-14 15:15:00 UTC
Updated	2022-05-24 18:18:00 UTC
Description	Zenario CMS 9.0.54156 is vulnerable to File Upload. The web server can be compromised by uploading and executing a w

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tribalsystems	Zenario	9.0.54156	All	All	All

References

Reference	Source	Link
Zenario CMS 9.0.54156 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecu
File upload to Remote Code Execution on Zenario CMS 9.0.54156 by Minh Quang Nguyen Medium	MISC	minhng22.medium
Upload file to RCE in Zenario CMS 9.0.54156 · Issue #2 · hieuminhvn/Zenario-CMS-9.0-last-version · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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