



CVE-2023-36212

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

Summary

CVE	CVE-2023-36212
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-03 02:15:00 UTC
Updated	2023-08-05 03:49:00 UTC
Description	File Upload vulnerability in Total CMS v.1.7.4 allows a remote attacker to execute arbitrary code via a crafted PHP file to the

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Totalcms	Total Cms	1.7.4	All	All	All

References

Reference	Source	Link	Tags
Total CMS 1.7.4 - Remote Code Execution (RCE) - PHP webapps Exploit	MISC	www.exploit-db.com	
Total CMS 1.7.4 Shell Upload ≈ Packet Storm	MISC	packetstormsecurity.com	
GitHub - capture0x/Total-CMS-EXPLOIT: Total CMS 1.7.4 Shell Upload	MISC	github.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.

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