CVE-2020-28872

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-28872
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-12 14:15:00 UTC
Updated	2024-01-26 16:46:00 UTC
Description	An authorization bypass vulnerability in Monitorr v1.7.6m in Monitorr/assets/config/_installation/_register.php allows an una

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Monitorr	Monitorr	1.7.6m	All	All	All
Application	Monitorr Project	Monitorr	1.7.6m	All	All	All

References

Reference	Source	Link
How the White-Box hacking works: Authorization Bypass and Remote Code Execution in Monitorr 1.7.6 – Lyhin's Lab	MISC	lyhinslab
Monitorr 1.7.6m Bypass / Information Disclosure / Shell Upload ≈ Packet Storm	MISC	packetsto
Monitorr 1.7.6m - Authorization Bypass - PHP webapps Exploit	MISC	www.exp
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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