CVE-2021-40903

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

Summary

CVE	CVE-2021-40903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-17 14:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	A vulnerability in Antminer Monitor 0.50.0 exists because of backdoor or misconfiguration inside a settings file in flask serve

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Antminer Monitor Project	Antminer Monitor	0.50.0	All	All	All

References

Reference	Source	Link
GitHub - anselal/antminer-monitor: Cryptocurrency ASIC mining hardware monitor using a simple web interface	MISC	github.com
packetstormsecurity.com/files/164048/Antminer-Monitor-0.5.0-Authentication-Bypass.html	MISC	packetstormse
Antminer Monitor 0.5.0 - Authentication Bypass - Multiple webapps Exploit	MISC	www.exploit-d
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.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 registred 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