CVE-2021-24023

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

Summary

CVE	CVE-2021-24023
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-03 15:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	An improper input validation in FortiAI v1.4.0 and earlier may allow an authenticated user to gain system shell access via a

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Fortinet	Fortiai 3500f	-	All	All	All
Operating System	Fortinet	Fortiai Firmware	All	All	All	All

References

Reference	Source	Link	Tags
FortiAI - OS command injection due to improper input sanitization | FortiGuard	CONFIRM	fortiguard.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.

Free CVE JSON API cve.report/api

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