CVE-2022-31814

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-31814
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-05 16:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	pfSense pfBlockerNG through 2.1.4_26 allows remote attackers to execute arbitrary OS commands as root via shell metacl

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgate	Pfblockerng	All	All	All	All

References

Reference	Source	Link	Tags
pfBlockerNG 2.1.4_26 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
pfBlockerNG Unauth RCE Vulnerability - IHTeam Security Blog	MISC	www.ihteam.net	
Packages — pfBlocker-NG Package | pfSense Documentation	MISC	docs.netgate.com	
pfSense pfBlockerNG 2.1.4_26 Shell Upload ≈ Packet Storm	MISC	packetstormsecurity.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.

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