



CVE-2018-20799

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

Summary

CVE	CVE-2018-20799
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-01 15:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In pfSense 2.4.4_1, blocking of source IP addresses on the basis of failed HTTPS authentication is inconsistent with blockir

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgate	Pfsense	2.4.4	p1	All	All
Application	Netgate	Pfsense	2.4.4	p1	All	All

References

Reference	Source	Link	Tags
Bug #9223: SSHGUARD doesn't work as expected - pfSense - pfSense bugtracker	MISC	redmine.pfsense.org	Exploit, Issue Track
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, 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)