CVE-2020-10797

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10797
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-29 14:15:00 UTC
Updated	2020-05-01 14:42:00 UTC
Description	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	T
Validation and encoding for Ping and Traceroute. Fixes #10355 · pfsense/pfsense@cc3990a · GitHub	MISC	github.com	F
Bug #10355: diag_ping.php: Potential XSS via Hostname parameter - pfSense - pfSense bugtracker	MISC	redmine.pfsense.org	Is
Releases — 2.4.5 New Features and Changes | pfSense Documentation	CONFIRM	docs.netgate.com	F
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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