



CVE-2023-27100

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-27100
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 23:15:00 UTC
Updated	2023-04-10 20:15:00 UTC
Description	Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v2

Risk And Classification

Problem Types: CWE-307

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgate	Pfsense Plus	22.05.1	All	All	All
Application	Pfsense	Pfsense	2.6.0	All	All	All

References

Reference	Source	Link
docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc	MISC	docs.netgate.com
Bug #13574: Extra remote address information can confuse ``sshguard`` - pfSense - pfSense bugtracker	MISC	redmine.pfsense.org
pfSenseCE 2.6.0 Protection Bypass ~ Packet Storm	MISC	packetstormsecurity.com
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.

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 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](#)