



# CVE-2020-21487

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-21487
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-04 15:15:00 UTC
<b>Updated</b>	2023-04-10 18:09:00 UTC
<b>Description</b>	Cross Site Scripting vulnerability found in Netgate pfSense 2.4.4 and ACME package v.0.6.3 allows attackers to execute ar

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Netgate</a>	<a href="#">Pfsense</a>	2.4.4	-	All	All
Application	<a href="#">Netgate</a>	<a href="#">Pfsense Acme Package</a>	0.6.3	All	All	All

## References

Reference	Source	Link
Prevent ACME output from being interpreted as HTML. Fixes #9888 · pfsense/FreeBSD-ports@a6f443c · GitHub	MISC	<a href="#">github.com</a>
Bug #9888: ACME output sent to browser without encoding - pfSense Packages - pfSense bugtracker	MISC	<a href="#">redmine.pfsense.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**