

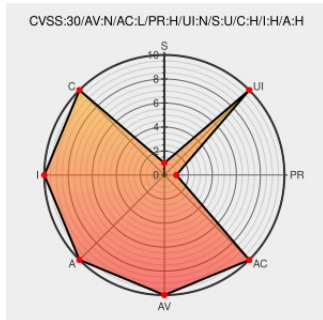


CVE-2018-4021

Published on: 12/03/2018 12:00:00 AM UTC

Last Modified on: 06/07/2022 05:22:00 PM UTC

CVE-2018-4021

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Pfsense](#) from [Netgate](#) contain the following vulnerability:

An exploitable command injection vulnerability exists in the way Netgate pfSense CE 2.4.4-RELEASE processes the parameters of a specific POST request. The attacker can exploit this and gain the ability to execute arbitrary commands on the system. An attacker needs to be able to send authenticated POST requests to the administration web interface. Command injection is possible in the `powerd\_battery\_mode` POST parameter.

CVE-2018-4021 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cisco](#) **Netgate** - **Netgate pfSense** version **Netgate pfSense CE 2.4.4-RELEASE**

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgate	Pfsense	2.4.4	All	All	All
Application	Netgate	Pfsense	2.4.4	All	All	All
cpe:2.3:a:netgate:pfsense:2.4.4:*****:						
cpe:2.3:a:netgate:pfsense:2.4.4:*****:						

No vendor comments have been submitted for this CVE