



CVE-2017-1000479

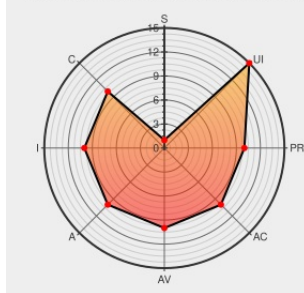
Published on: 01/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000479

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

pfSense versions 2.4.1 and lower are vulnerable to clickjacking attacks in the CSRF error page resulting in privileged execution of arbitrary code, because the error detection occurs before an X-Frame-Options header is set. This is fixed in 2.4.2-RELEASE. OPNsense, a 2015 fork of pfSense, was not vulnerable since version 16.1.16 released on June 06, 2016. The unprotected web form was removed from the code during an internal security audit under "possibly insecure" suspicions.

CVE-2017-1000479 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Clickjacking vulnerability in CSRF error page	Pfsense	MISC

Clickjacking vulnerability in CSRF error page pfSense - Security Advisories and Insights - Securify B.V.	Exploit Third Party Advisory www.securify.nl text/html	MISC www.securify.nl/en/advisory/SFY20171101/clickjacking-vulnerability-in-csrf-error-page-pfsense.html
pfSense 2.4.2-RELEASE-p1 and 2.3.5-RELEASE-p1 now available	Third Party Advisory www.netgate.com text/html	MISC www.netgate.com/blog/pfsense-2-4-2-release-p1-and-2-3-5-release-p1-now-available.html
csrf: tighten csrf code paths a little · opnsense/core@d218b22 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/opnsense/core/commit/d218b225
oss-security - Clickjacking vulnerability in CSRF error page pfSense	Exploit Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20171122 Clickjacking vulnerability in CSRF error page pfSense
Prevent Clickjacking in CSRF error page · pfsense/pfsense@386d89b · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/pfsense/pfsense/commit/386d89b07
Releases — 2.4.2 New Features and Changes pfSense Documentation	Issue Tracking Vendor Advisory doc.pfsense.org text/html	MISC doc.pfsense.org/index.php/2.4.2_New_Features_and_Changes

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	All	All	All	All
Application	Opnsense Project	Opnsense	All	All	All	All
Application	Opnsense Project	Opnsense	All	All	All	All
<pre>cpe:2.3:a:netgate:pfsense:*. *.*.*.*.*.*.*.*:</pre>						
<pre>cpe:2.3:a:opnsense_project:opnsense:*. *.*.*.*.*.*.*.*:</pre>						
<pre>cpe:2.3:a:opnsense_project:opnsense:*. *.*.*.*.*.*.*.*:</pre>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)