dharmeshbaskaran / **CVE-2020-19201**

Created last year

☆ Star

<> Code Revisions 1

Authenticated Stored XSS in pfSense 2.4.4-p2

CVE-2020-19201

```
pfSense-SA-19_03.webgui                                     Security Advisory
                                                                      pfSense

Topic:          XSS vulnerability in the WebGUI

Category:       pfSense Base System
Module:         webgui
Announced:      2019-05-20
Credits:        Dharmesh Baskaran -- https://www.linkedin.com/in/dharmeshbaskaran
CVE ID:         CVE-2020-19201
Affects:        pfSense software versions <= 2.4.4-p2
Corrected:      2019-05-03 19:24:43 UTC (pfSense/master, pfSense 2.5.0)
                2019-05-03 19:24:43 UTC (pfSense/RELENG_2_4_4, pfSense 2.4.4-pX)
                The latest revision of this advisory is available at
URL:            https://pfsense.org/security/advisories/pfSense-SA-19_03.webgui.asc
                https://redmine.pfsense.org/issues/9499


0.   Revision History

v1.1  2021-05-20 Added CVE ID
v1.0  2019-05-20 Initial SA draft

I.   Background

pfSense® software is a free network firewall distribution based on the
FreeBSD operating system.  The pfSense software distribution includes third-
party free software packages for additional functionality, and provides most of
the functionality of common commercial firewalls.

The majority of users of pfSense software have never installed or used a stock
FreeBSD system.  Unlike similar GNU/Linux-based firewall distributions, there
is no need for any UNIX knowledge.  The command line is never used, and there
is no need to ever manually edit any rule sets. Instead, pfSense software
includes a web interface for the configuration of all included components.
Users familiar with commercial firewalls will quickly understand the web
interface, while those unfamiliar with commercial-grade firewalls may encounter
a short learning curve.

II.  Problem Description

A Cross-Site Scripting (XSS) vulnerability was found in
status_filter_reload.php, a page in the pfSense software WebGUI, on version
2.4.4-p2 and earlier.

The page did not encode output from the filter reload process, and a stored XSS
was possible via the descr (description) parameter on NAT rules.

III. Impact

Due to the lack of proper encoding on the affected parameters susceptible to
XSS, arbitrary JavaScript could be executed in the user's browser. The user's
session cookie or other information from the session may be compromised.

IV.  Workaround

No workaround. To help mitigate the problem on older releases, use one or more
of the following:
* Do not give firewall administrators access to pages or functions which allow
  writing arbitrary files to the firewall.
* Limit access to the affected pages to trusted administrators only.
* Do not log into the firewall with the same browser used for non-
  administrative web browsing.

V.   Solution

Users can upgrade to version 2.4.4-p3 or later. This upgrade may be performed in
the web interface or from the console.

  See https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide.html

Users may also apply the relevant revisions below using the System Patches
package to obtain the fix.

  See https://docs.netgate.com/pfsense/en/latest/development/system-patches.html

VI.  Correction details

The following list contains the correction revision commit ID for each
affected item.
```

```

Branch/path                                                         Revision
- - -------------------------------------------------------------------------
pfSense/master                     1af9400d594cd183d011f22fa9b3a7630570a250
pfSense/RELENG_2_4_4               41c9fac85c3ff621665bd7fa7b9af497bc16fd3a
- - -------------------------------------------------------------------------

VII. References

<URL:https://redmine.pfsense.org/issues/9499>
<URL:https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide.html>
<URL:https://docs.netgate.com/pfsense/en/latest/development/system-patches.html>
```