-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

==========
pfSense-SA-25_03.webgui Security Advisory
pfSense

Topic: Potential XSS in AutoConfigBackup backup list

Category: pfSense Base System
Module: webgui
Announced: 2025-05-16
Credits: Github user NavyTitanium
CVE ID: CVE-2024-57273
Affects: pfSense Plus software versions < 25.07
pfSense CE software versions < 2.8.0
Corrected: 2024-12-12 12:23:41 UTC (pfSense Plus master, 25.07)
2024-12-12 12:23:41 UTC (pfSense CE master, 2.8.0)

0. Revision History

v1.1 2025-07-02 Updated pfSense Plus software version numbers
v1.0 2025-05-16 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.

pfSense® Plus is the productized version of pfSense software from Netgate®, previously referred to as pfSense Factory Edition (FE). It is available to Netgate appliance and CSP customers.

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

The page at services_acb.php displays the "reason" string when listing backup entries from the server without encoding.

This problem is present on pfSense Plus version 24.11, pfSense CE version 2.7.2, and earlier versions of both.

III. Impact

If a backup entry on the server contains a "reason" string containing malicious content, it may be rendered by the browser.

The AutoConfigBackup feature on pfSense software encodes the "reason" string when creating a backup, but this encoding is performed by the client so it may not always happen as expected. For example, if a malicious actor uses their own code to create backup entries on the server for the Device Key of the target.

Due to the lack of encoding on the "reason" content, when services_acb.php lists remote backups stored on the AutoConfigBackup server can be susceptible to XSS.

There is a potential that 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

To help mitigate the problem on older releases, use one or more of the following:

* Do not allow any untrusted parties to know the AutoConfigBackup Device Key of a host running pfSense software.
* Do not log into the firewall with the same browser used for non-administrative web browsing.

V. Solution

Users can upgrade to pfSense Plus software version 25.07 or later, or pfSense CE software versions after 2.8.0 when available. 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 on pfSense Plus version 24.11 and pfSense CE version 2.7.2 may apply the fix from the recommended patches list in the System Patches package.

Users may also manually apply the relevant revisions below using the System Patches package on earlier versions, or by manually making similar changes to the affected files if the patches do not apply directly.

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
plus/plus-master	84d8eddf87607e0f9dcc313bcaad4db67e4f3750
pfSense/master	84d8eddf87607e0f9dcc313bcaad4db67e4f3750

VII. References

<URL:https://redmine.pfsense.org/issues/15927>
<URL:https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide.html>
<URL:https://docs.netgate.com/pfsense/en/latest/development/system-patches.html>

The latest revision of this advisory is available at
<URL:https://docs.netgate.com/downloads/pfSense-SA-25_03.webgui.asc>
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEE40XvjEU56XSUPIMdE7mH/ZIU+NoFAmhleAYACgkQE7mH/ZIU
+NoImhAArbhEVgzm5sDAWGL4FDBvPLgS/aw+Nb0oTnq7BBrcNCMVMrnvE+p5zqkm
EZ9xS72JTIxNRdSriI6QMYePSxG5i5CFkfzaAsBa8v9vcUIB8w3K2SnTGO2H6c0Q
Mke9aCkBn6JdAVVKMf2XVs6qrXtIcfehoUnvrGOoZcdZeFyjZda6mVjOH4WPm3Vi
pDwuQmEiZJTCQ9pr2TXzBPSZleoD+vS3qenYUymBhkUDROCb6wJq9ggbW8iK7AtY
193NdaROUjvTgvC/amrnbO7DG31pRdhnxElk6oV0Ryn4QruL22jwj+Kezvm6GOIO
Jtkv2EO7GS3u17gWJ60ZEfK48+N7BAYwdxObcjY/y6fu3CpioYpqyCdMzZ08YYo9
JrRtKfVY4LjbYvrRU7qH7haCQ2Z0SLvhoVbT1bqw5KYyzqSpyLK8V1JLn7AyuUPB
FEci8e5EuBXZU8nmFkNEgLKtOWlMobL3/kQKid7JpE7YVUachxtks4v5MXfv8XJo
X4nlb50UFOu4F9WrdobEwhPwkCH58KJ+KSG0fBHjLOGVIoQpV2+/V6W25OB7mX2X
/vH6pOSQ62Ki/iVMTuQguS1DZk33kiLwt6dg/a06On6aaX8pMFh1ei9Os6QrRdJP
YqmtFcDd6MPfDO+RlmeDuXx0arcd/W30DkxcBnyWLFn9lxxcHLo=

```
=Y2PZ
-----END PGP SIGNATURE-----
```