



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)



XSS stored in PFSense 2.5.0 CVE-2021-27933

From: William Costa <william.costa () gmail com>

Date: Tue, 27 Apr 2021 15:13:24 -0300

I. VULNERABILITY

Store XSS Attacks vulnerabilities in PFSense Version 2.5.0

II. BACKGROUND

The pfSense project is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality. Through this package, system pfSense software is able to provide most of the functionality of common commercial firewalls, and many times more.

III. DESCRIPTION

Has been detected a Stored XSS vulnerability in PFSense. The code injection is done through the parameter "Description" in the page "/services_wol_edit.php?id=0"

IV. PROOF OF CONCEPT

The application does not validate the parameter "Description" correctly when run Wake All Devices.

First add script in field "Description"

After Run

Wake All Devices

/services_wol.php?wakeall=true

V. BUSINESS IMPACT

An attacker can execute arbitrary HTML or script code in a targeted user's browser, that allows the execution of arbitrary HTML/script code to be executed in the context of the victim user's browser.

VI. SYSTEMS AFFECTED

Tested PFSense 2.5.0

VII. SOLUTION

All data received by the application and that can be modified by the user, before making any kind of transaction with them must be validated correctly Upgrade 2.5.1

By William Costa

william.costa () gmail com

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

XSS stored in PFSense 2.5.0 CVE-2021-27933 *William Costa (Apr 27)*



Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License

