phpIPAM 1.4.4 – Stored XSS

Summary

Name	phpIPAM 1.4.4 – Stored XSS

Fixed versions	1.4.5
State	Public
Release date	2022-01-18

Vulnerability

Kind	Stored cross-site scripting (XSS)
Rule	010. Stored cross-site scripting (XSS)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
CVSSv3 Base Score	4.8
Exploit available	No
CVE ID(s)	CVE-2022-23045

Proof of Concept

Steps to reproduce:

XSS:

1. Go to `"http://192.168.1.5/phpipam/index.php?
page=administration&section=settings"`.
2. Update the "Site Title" parameter with `" autofocus onfocus=alert(1)>`.
3. Click on 'Save'.
4. If a user visits the settings page the javascript code will be rendered.

Open redirect:

1. Go to `"http://192.168.1.5/phpipam/index.php?`
   `page=administration&section=settings"`.
2. Update the "Site Title" parameter with `0;url=https://google.com"`
   `http-equiv="refresh"`.
3. Click on 'Save'.
4. If a user reloads the page, they will be redirected to
   `https://google.com`.

System Information

- Version: phpIPAM IP address management v1.4.4.
- Operating System: Linux.
- Web Server: Apache
- PHP Version: 7.4
- Database and version: Mysql

An updated version of phpIPAM is available at the vendor page.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks`.

References

Vendor page https://phpipam.net/

Patched version https://github.com/phpipam/phpipam/releases/tag/v1.4.5

Timeline

2022-01-06
Vulnerability discovered.

2022-01-07
Vendor contacted.

2022-01-07
Vendor replied acknowledging the report.

2022-01-17
Vulnerability patched.

2022-01-18
Public Disclosure.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Contact

Service Status **-** Terms of Use **-** Privacy Policy **-** Cookie Policy