Home / Advisories / PeTeReport 0.5 Stored XSS (Markdown)

PeTeReport 0.5 - Stored XSS (Markdown)

Summary

Affected versions	Version 0.5
Fixed versions	Version 0.7
State	Public
Release date	2022-02-23

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-2022-25220

Proof of Concept

Steps to reproduce

1. Click on 'Add Product'.

2. Insert the following PoC inside the product description.

```
[XSS](javascript:alert(1))
```

3. Click on 'Save Product'.

4. If a user visits the product and click on the link in the description the javascript code will be rendered.

System Information

- Version: PeteReport Version 0.5.
- Operating System: Docker.
- Web Server: nginx.

Exploit

There is no exploit for the vulnerability but can be manually exploited.

Mitigation

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

References

Vendor page https://github.com/1modm/petereport

Issue https://github.com/1modm/petereport/issues/35

Timeline

✓ 2022-02-08
Vulnerability discovered.

✓ 2022-02-08
Vendor contacted.

✓ 2022-02-09
Vendor replied acknowledging the report.

- 2022-02-28
  Vulnerability patched.
- 2022-02-23
  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

Careers

Advisories

FAQ

Documentation

Contact