Stored Cross-Site Scripting (XSS) on Schedule Maintenance "Title" parameter in librenms/librenms

1

Valid Reported on Sep 15th 2022

Description

Stored Cross-Site Scripting (XSS) vulnerability in LibreNMS v22.8.0 allows attackers to execute arbitrary javascript code in the browser affected from function of "Schedule Maintenance" in "Title" parameter.

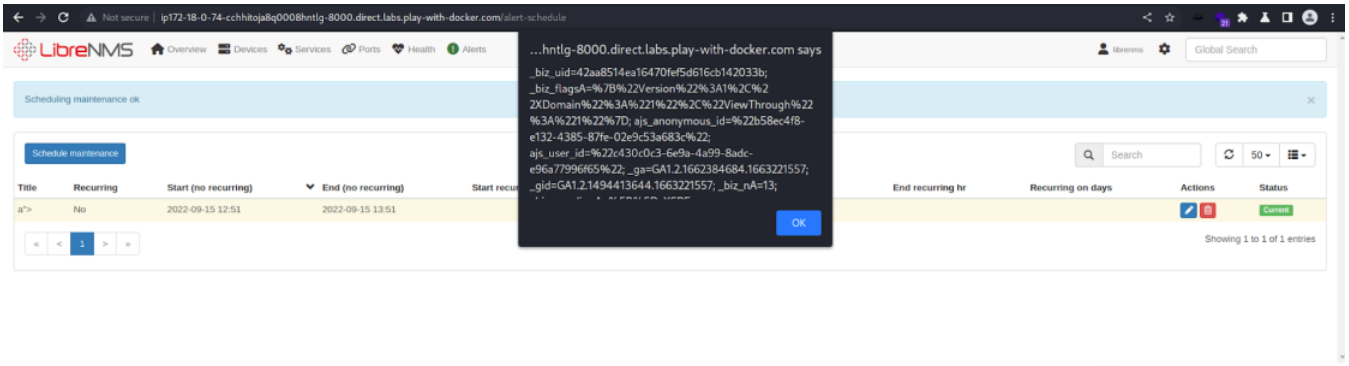
Proof of Concept

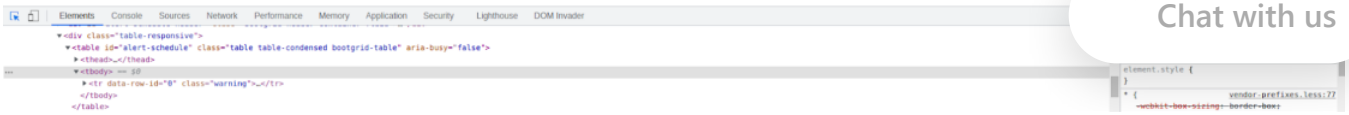
1 - Click "Alerts" > Click "Schedule Maintenance" from the dropdown
2 - Create a new schedule by clicking "Schedule Maintenance" green button
3 - Under "Title" , use payload below

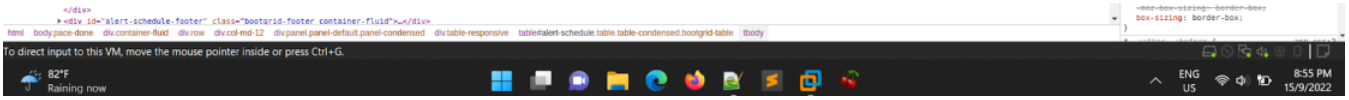
```
saitamang"><iMg SrC="x" oNeRRor="alert(document.cookie);">
```

4 - Saved the new schedule by clicking the green button name "Schedule Maintenance"
5 - XSS will prompt afterwards.

PoC Image







PoC Video

https://drive.google.com/file/d/1sWsIJsENvwhig5notCKWh2C6_h-MvBN0/view?usp=

Impact

This vulnerability allows attackers to hijack the user's current session, steal relevant information, deface website or direct users to malicious websites and allows attacker to use for further exploitation.

CVE
CVE-2022-3231
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (5.6)

Registry
Other

Affected Version
22.8.0

Visibility
Public

Status
Fixed

Found by

Saitamang
@saitamang
unranked

Fixed by

Tony Murray

@murrant

maintainer

This report was seen 861 times.

We are processing your report and will contact the **librenms** team within 24 hours. 2 months ago

Saitamang modified the report 2 months ago

Saitamang modified the report 2 months ago

We have contacted a member of the **librenms** team and are waiting to hear back 2 months ago

Tony Murray validated this vulnerability 2 months ago

Saitamang has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Tony Murray marked this as fixed in **22.9.0** with commit **080500** 2 months ago

Tony Murray has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation