huntr

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

0

✔ Valid   Reported on Feb 18th 2022

Stored-xss is possible when adding a rule.

Create a new Alert Rule (like below) and adjust the query like below with the following payload

```
"><img src=x onerror=alert(document.cookie)>
```

Alert Rule :: 🗐 Docs

Main   Advanced

Rule name	test

Import from ▾

AND OR   + Add rule ⊕ Add group

access_points.accesspoint_id ▾   equal ▾   ✖ Delete

"><svg/onload=alert(docu

Severity   Warning ▾

Max alerts   1   Delay 1m   Interval 5m

Mute alerts   OFF   Invert rule match   OFF

Recovery alerts   ON

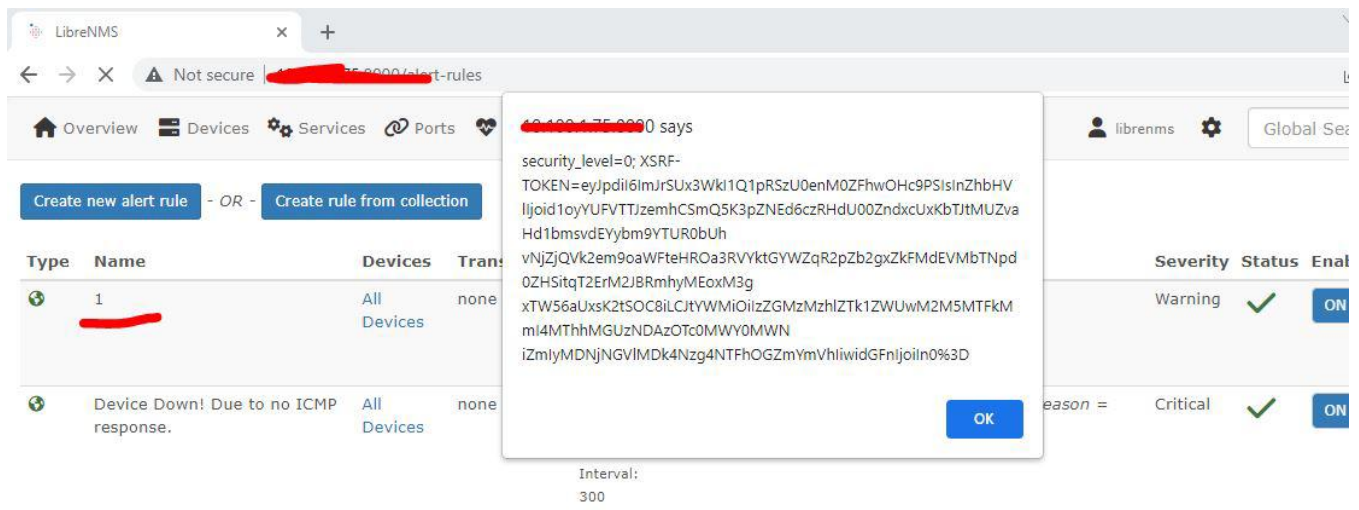Match devices, groups and locations list   Devices, Groups or Locatic   All devices except in list   OFF

Transports   Transport/Group Name

Procedure URL

Save Rule

Save the rule and see a xss-pop up.

Chat with us

security_level=0; XSRF-
TOKEN=eyJpdiI6ImJrSUx3WkI1Q1pRSzU0enM0ZFhwOHc9PSIsInZhbHV
lIjoid1oyYUFVTTJzemhCSmQ5K3pZNEd6czRHdU00ZndxcUxKbTJtMUZva
Hd1bmsvdEYybm9YTUR0bUh
vNjZjQVk2em9oaWFteHROa3RVYktGYWZqR2pZb2gxZkFMdEVMbTNpd
0ZHSitqT2ErM2JBRmhyMEoxM3g
xTW56aUxsK2tSOC8iLCJtYWMiOiIzZGMzMzhlZTk1ZWUwM2M5MTFkM
mI4MThhMGUzNDAzOTc0MWY0MWN
iZmIyMDNjNGVlMDk4Nzg4NTFhOGZmYmVhIiwidGFnIjoiIn0%3D

OK

CVE
CVE-2022-0772
(Published)

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

Severity
Medium (4.7)

Visibility
Public

Status
Fixed

Found by

ribersec

@ribersec

unranked

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

We have contacted a member of the **librenms** team and are waiting to hear back 9 months ago

Chat with us

Neil Lathwood modified the report 9 months ago

ribersec modified the report 9 months ago

We have sent a follow up to the **librenms** team. We will try again in 7 days. 9 months ago

Neil Lathwood modified the report 9 months ago

Neil Lathwood modified the report 9 months ago

Neil Lathwood validated this vulnerability 9 months ago

ribersec has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Neil Lathwood marked this as fixed in **22.2.2** with commit **703745** 9 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

part of 418sec

company

about

Chat with us

leaderboard

team

FAQ

contact us

terms

privacy policy

Chat with us