

Forum:[Hack Forums](#)

Thread: [CVE-2017-3169 - Apache 2.2.22 - Exploit](#)

GLXBX - August 1, 2018, 2:52 am

Hi,

I want to get into a website which is still using Apache 2.2.22 together with PHP 5.4.45.
Now i've checked for any exploits available to use and one of them which looks promising is the CVE-2017-3169:

Quote:The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_ssl. Review your web server configuration for validation. mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

There is an exploit on GitHub:

https://github.com/gottburgm/Exploits/blob/master/CVE-2017-3169/CVE_2017_3169.pl

But when i try to run it on the external IP adres it says it can't find the local apache directory.
Everywhere on the internet it says it's an exploit for remote hackers, but why the local directory?

Anybody knows how to use this exploit on a remote webserver?

Thanks!

Overdosed - August 1, 2018, 7:37 pm

Just to make sure... Have you port forwarded? Have you tested the port connection? canyouseeme.org should help you.

Also based on the exploit make sure these settings are set.

```
my $apache_install = "";  
my $host = "127.0.0.1";  
my $http_port = 9080;  
my $https_port = 9443;  
my $debug = 0;
```

Gee4rce - August 2, 2018, 12:52 pm

It is indeed a bit odd,
according to CVSSv3 vector it is marked as a remote exploit
as the vector starts with AV:N ... which stands for "Network",
"Local" would have it's own short form AV:L, but vector in security advisory shows it's a remote exploit.

So either it is wrongly calculated,
or we are missing something maybe.

Another Option could be that you need to be on the same Network,
or dealing with vhosts on shared hosting. But then the CVSSv3 vector
would still be wrong, as then it would have to be AV:A, for "Adjacent Network".

Anyways,
incase it is a remote exploit, you'd have to set the \$apache_install variable
to the path of the apache installation, i.e. "/usr/local/apache2" and the ip of the target.
You could test it with local first, and next on 2 virtual machines, if that works then test
with a remote target again.

If anyone wants to check the CVSSv3 vector, here's a link:

<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L>

(you can mouse over the single fields, it will popup an explanation incase anyone wants to know
more).

Cheers, Gee.