

Forum:[Hack Forums](#)

Thread: [\[Need Help\] Heap Buffer/Overflow \(Remote\)](#)

Gh0st_Dragon - October 15, 2017, 12:19 am

Hello

I got the permission to pentest a VirtualMaschine Server from a Friend and has found a vulnerability.

He uses an old version of nginx (1.4.6) and after search a vulnerability on databases it said

Quote:Schwachstelle : nginx 1.4.6
80/tcp open http nginx 1.4.6 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-server-header: nginx/1.4.6 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).

A bug in the experimental SPDY implementation in nginx was found, which might allow an attacker to cause a heap memory buffer overflow in a worker process by using a specially crafted request, potentially resulting in arbitrary code execution (CVE-2014-0133).

Now i search an Exploit to get Root Acces on the server , to Upload a html site

where says "Pentesting Succesfull"

i write a Protokoll about it.
I have the permission for Training on his server runs a Hacking Challenge.

But i must send the Heap Buffer/Overflow via Remote its no problem then he see my IP or something he know i try to get acces.

I Use : Kali 2.0 with Gh0stSec Linux , Orginal Kali , and Own tools.

but i am new in writting own Exploits (i have only Knowlege in Python2 and Python3)

I Hope someone can help me.

Greetings
Gh0st_Dragon

CyberStrike - October 15, 2017, 7:53 pm

Well does it have nginx compiled with --with-http_spdy_module ? If it isn't then keep searching.

Gh0st_Dragon - October 16, 2017, 6:17 am

I think he has compiled with it.

i am new in learning pentesting and can train on his server.
So i know he runs only

SSH on port 22 and nginx 1.4.6 on port 80.

i know he runs the system on a VM for pentesting
now i search informations how to get acces.

CyberStrike - *October 16, 2017, 12:13 pm*

Well you will want to use wappalyzer or check the server headers then maybe chrome and view the results for a SPDY sessions via

Code chrome://net-internals/#spdy
Also you can check at
Code spdycheck.org

Gh0st_Dragon - *November 9, 2017, 12:41 pm*

Okay , i have check it
he haven't compiled it with SPDY
i have with his allow make with metasploit a "Hail Mary" attack
nothing happend xD

thanks for all help
ui must search another way

CyberStrike - *November 9, 2017, 1:00 pm*

(Nov 9, 2017 01:41 PM)Gh0st_Dragon Wrote: [\[CITE\]](#) Okay , i have check it
he haven't compiled it with SPDY
i have with his allow make with metasploit a "Hail Mary" attack
nothing happend xD

thanks for all help
ui must search another way
? Hail Mary ?

Geez that sure was obvious you set off not only the alarms and raised a big red flag but also shot off fireworks to any would be defender. Sometimes that happens I guess keep searching you will literally feel on top of the world when you do get into the machine. Look for low hanging fruit such as anonymous ftp something.