Vulnerability Assessment Report

Ime i prezime: Balsa Bulatović
Datum: 24.11.2025
Scan Tool: Nessus (Docker version — oracle-latest)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

CVE ID: CVE-1999-0511

Opis

Na hostu je omogućeno **IP forwarding** (prosleđivanje IP paketa).
Kada je ova funkcionalnost aktivna, sistem se može koristiti kao ruter i automatski prosleđivati mrežne pakete između interfejsa. Ako host nije namenjen da bude ruter, ovo predstavlja sigurnosni rizik jer omogućava:

- neautorizovanu manipulaciju mrežnim saobraćajem,
- olakšavanje tehnika kao što su MITM (Man-in-the-Middle), ARP spoofing i paketni tunelovani napadi.

Očekivano stanje: IP forwarding bi trebalo da bude **onemogućen** na svim hostovima koji nisu ruteri.

Port: N/A
Protokol: N/A
Tip ranjivosti: Mrežna konfiguraciona slabost (Firewall/Network Exposure)

---

2. CVSS skor

CVSS skor: 6.5 (Medium)

Vektor

`CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L`

Objašnjenje komponenti

- **AV:N (Network)** – napad se izvodi udaljeno, preko mreže.
- **AC:L (Low)** – exploitation zahteva minimalan napor.
- **PR:L (Low Privileges)** – napadač mora imati neki pristup mrežnom segmentu ili hostu.
- **UI:N (None)** – nije potrebna interakcija žrtve.
- **S:C (Changed)** – kompromitacija može uticati na druge sisteme u mreži.
- **C:L (Low)** – napadač može delimično pristupiti ili ometati saobraćaj.
- **I:L (Low)** – moguće menjanje ili preusmeravanje paketa.
- **A:L (Low)** – delimičan uticaj na dostupnost, posebno kod tunelovanih napada.

Opravdanje

Omogućeno IP forwarding može biti iskorišćeno kao deo kompleksnijeg napada (npr. MITM, spoofing, tunelovanje), ali samo po sebi ne dovodi direktno do kompromitacije sistema.
Zbog toga rizik ostaje srednji, ali postaje ozbiljan u kombinaciji sa drugim mrežnim ranjivostima.

---

3. Dostupnost eksploita

Postoji javno dostupan eksploit: Ne (specifičan eksploit nije primenjiv)

Objašnjenje

Ovo nije programska ranjivost, već **nesigurna mrežna konfiguracija** OS-a.
IP forwarding je legitiman kernel feature i predstavlja rizik samo kada je uključen na sistemima gde to nije predviđeno.

Napadi koji koriste omogućen IP forwarding uključuju:

- **MITM** u kombinaciji sa ARP spoofingom,
- **traffic redirection**,
- **firewall bypass**,
- **neovlašćeno rutiranje** u mreži.

Zbog toga se ova slabost kategorizuje kao **konfiguraciona**, a ne kao exploitabilna ranjivost.

---

4. Analiza uzroka (root cause)

Uvođenje greške (Konfiguracija OS-a)

Root cause je ručno ili automatski omogućavanje IP prosleđivanja u sistemu.
Na Linux sistemima IP forwarding je kontrolisan preko:

```
/proc/sys/net/ipv4/ip_forward
```

Ovo polje ima vrednost:

- `0` → forwarding isključen
- `1` → forwarding uključen

Na Metasploitable3 VM-u ip_forward je poznato često uključen radi testnih scenarija.

Primer konfiguracije

Nessus output pokazuje:

```
Detected local MAC address: 66:4d:2e:b9:10:9f
Response from local MAC address: 66:4d:2e:b9:10:9f

Detected gateway MAC address: 0e:e7:23:47:31:70
Response from gateway MAC address: 0e:e7:23:47:31:70
```

Podudaranje odgovora na ARP upite potvrđuje da host rutira pakete.

---

5. Preporuke za mitigaciju

Vendor Fix / Patch: Nije potrebna zakrpa (konfiguracioni problem)

Mitigation Strategy

Linux

Isključiti IP forwarding odmah:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

Za trajno gašenje u `/etc/sysctl.conf`:

```
net.ipv4.ip_forward = 0
```

Primena:

```
sysctl -p
```

Windows

U registru postaviti:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter =
0
```