

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: *N/A - End-of-Life (EOL) operativni sistem*
(Ranjivost se ne vezuje za jedan CVE, već obuhvata ceo OS koji više ne prima zakrpe.)

Opis

Host koristi operativni sistem **Ubuntu Linux 14.04.x**, koji je zvanično dostigao **End of Life (EOL)** 30. aprila 2019. godine.

Po završetku perioda podrške, proizvođač više ne obezbeđuje:

- bezbednosne zakrpe,
- sigurnosne ispravke,
- tehničku podršku,
- ažuriranja jezgra i sistemskih paketa.

Korišćenje EOL OS-a znači da sistem može sadržati veliki broj javno poznatih i aktivno eksploatisanih ranjivosti, bez mogućnosti nadogradnje putem regularnih sigurnosnih kanala.

OS: Ubuntu Linux 14.04
Datum završetka sigurnosne podrške: 30. april 2019.
Starost od EOL: više od 6 godina (Nessus: *6+ years*)
Port detekcije: 80/tcp (HTTP banner identifikacija)
Tip ranjivosti: Unsupported / End-of-Life Operating System

2. CVSS skor

CVSS skor: 10.0 (Critical)

Vektor

Nessus navodi sledeće CVSS 3.0 i 2.0 vektore:

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

CVSS 2.0:
AV:N/AC:L/Au:N/C:C/I:C/A:C

Objašnjenje komponenti

- **AV:N (Network)** – napad se izvodi udaljeno.
- **AC:L (Low)** – napad ne zahteva posebne uslove.
- **PR:N (None)** – privilegije nisu potrebne.
- **UI:N (None)** – ne zahteva korisničku interakciju.
- **S:C (Scope: Changed)** – kompromitacija može uticati na druge komponente sistema.
- **C:H (High) / C:C (Complete)** – potpuni uticaj na poverljivost.
- **I:H (High) / I:C (Complete)** – potpuni uticaj na integritet.
- **A:H (High) / A:C (Complete)** – potpuni uticaj na dostupnost.

Opravljanje

Operativni sistem koji je dostigao EOL status ne poseduje nikakav mehanizam odbrane protiv novih ranjivosti.

Time se:

- akumuliraju sve ranjivosti otkrivene nakon EOL datuma,
- mnoge od njih imaju javno dostupne exploite,
- napadi su trivijalni i često automatizovani,

Zbog toga Nessus dodeljuje maksimalni CVSS skor **10.0**.

3. Dostupnost eksploita

Postoji javno dostupan exploit: Da

EOL sistem može sadržati **stotine** poznatih ranjivosti, uključujući:

- kernel RCE ranjivosti,
- privilege escalation,
- OpenSSL ranjivosti,
- zastarele biblioteke (glibc, bash, Python, PHP...).

Opis eksploita

Ne postoji jedan „specifičan“ exploit za EOL OS, već bukvalno *čitav ekosistem* ranjivosti.

Napadač može kompromitovati sistem korišćenjem:

- Metasploit modula za stari kernel,
- javno dostupnih exploit PoC-eva sa Exploit-DB,

Drugim rečima, kompromitacija je **trivijalna** jer proizvođač više ne izdaje zakrpe.

4. Analiza uzroka (root cause)

Uvođenje greške

Uzrok nije pojedinačni bug ili commit, već:

- **prestanka održavanja OS verzije**
- **potpun izostanak sigurnosnih ažuriranja**

Ubuntu 14.04 je aktivno podržavan do **30. aprila 2019.**, nakon čega:

- svi paketi su ostali bez zakrpa,
- novi CVE-ovi nisu zatvarani,
- postojeće ranjivosti nisu ispravljane.

5. Preporuke za mitigaciju

Dostupan Vendor Fix / Patch: Ne (jer OS više nije podržan)
Vendor ne pruža zakrpe niti Extended Security Maintenance za ovu verziju bez komercijalnog ugovora.

Mitigation Strategy

1. **Obavezna nadogradnja OS-a** na podržanu verziju Ubuntu-a (20.04, 22.04 ili novije).
2. Ako migracija nije odmah moguća:
 - postaviti VM u izolovani segment mreže (VLAN / subnet izolacija),
 - ograničiti sav dolazni saobraćaj firewall-om,
 - blokirati sve nepotrebne portove,
 - omogućiti intrusion detection (OSSEC, Wazuh).

Alternativni fix (privremeni)

Ako je nadogradnja odložena zbog kompatibilnosti:

- migracija servisa pojedinačno (Docker containerizacija),
- zamena zastarelih servisa novim verzijama bez menjanja celog OS-a,

Ovo je samo privremena mera. **EOL OS predstavlja visok rizik i mora biti zamenjen.**