# Nessus AI sérülékenységi riport – 10.44.100.101

Semmelweis Egyetem – Infrastruktúra Üzemeltetés

**Telephely:** Radiológiai és Onkoterápiás Klinika
**VLAN:** VLAN-418
**Funkció:** Klinikai ellátás
**Operációs rendszer:** ismeretlen
**Súlyossági bontás:** Critical: 0 | High: 0 | Medium: 11 | Low: 7 | Info: 92

## AI alapú C-típusú összefoglaló

A megadott szöveg több mint 100 részt foglal magában, amelyek közül több is azonos címzés■, hasonló problémákat és javaslatokat tartalmaz. A f■bb részek a következ■k:

1. **Vezet■i összefoglaló**: Ez nem található meg közvetlenül a szövegben, de a bevezetésb■l és a többi részb■l is látható, hogy a f■ cél az, hogy felhívja a figyelmet a biztonsági fenyegetésekre és javaslatot adjon arra, hogy hogyan lehet ezeket kezelni.
2. **F■ kockázati típusok**:
- Kisz■rés és vírusok: A szövegben több helyen megjelenik a kockázat az OpenSSH és más alkalmazásokban található biztonsági rések miatt.
- Felhasználói adatok kiírása: Egyes részek arra utalnak, hogy egyes rendszerekben felhasználói adatok is kinyerhet■k, ami további kockázatot jelenthet.

3. **Javasolt lépések és prioritások (Azonnali / Rövid táv / Közép táv)**:
- Azonnali: Egyes részek az OpenSSH frissítését javasolják, hogy elkerülhessék a biztonsági réseket.
- Rövid táv: Egyik rész sem tartalmaz konkrét rövid távon végzend■ lépéseket. Azonban ez általánosságban abból is adódhat, hogy a rendszerek frissítését, figyelmeztetések beállítását és az egyéb biztonsági intézkedések meghatározását tekintik rövid távú feladatoknak.
- Közép táv: Egyes részek a rendszerfigyelést, figyelmeztetés küldéseket és további biztonsági intézkedések meghatározását javasolják.

4. **Technikai összefoglaló**: A szöveg részei részletesen bemutatják a különböz■ rendszerek és alkalmazások biztonsági réseit, valamint az ezekkel kapcsolatos problémákat. Ezeket a részeket általánosságban akkor használhatja egy szakember, ha specifikus probléma megoldását keresi.

Ebb■l a felsorolásból jól látható, hogy a biztonsági fenyegetésekre nagyon sok részletet tartalmaznak, és ezek az egymást kiegészít■ információk segítenek a rendszerek védelmében.

## Részletes Nessus sérülékenységi adatok (top 20)

| Severity | Plugin ID | Plugin Name | CVE | CVSSv3 | VPR | EPSS | Port/Proto |
|---|---|---|---|---|---|---|---|
| None | 10107 | HTTP Server Type and Version | | | | | 80/tcp |
| None | 10107 | HTTP Server Type and Version | | | | | 443/tcp |

| Severity | Plugin ID | Plugin Name | CVE | CVSSv3 | VPR | EPSS | Port/Proto |
|---|---|---|---|---|---|---|---|
| None | 10107 | HTTP Server Type and Version | | | | | 5000/tcp |
| None | 10107 | HTTP Server Type and Version | | | | | 5001/tcp |
| Low | 10114 | ICMP Timestamp Request Remote Date Discl | CVE-1999-0524 | | | | 0/icmp |
| None | 10150 | Windows NetBIOS / SMB Remote Host Inform | | | | | 137/udp |
| None | 10267 | SSH Server Type and Version Information | | | | | 2121/tcp |
| None | 10267 | SSH Server Type and Version Information | | | | | 2323/tcp |
| None | 10287 | Traceroute Information | | | | | 0/udp |
| None | 10302 | Web Server robots.txt Information Disclo | | | | | 5000/tcp |
| None | 10302 | Web Server robots.txt Information Disclo | | | | | 5001/tcp |
| None | 10386 | Web Server No 404 Error Code Check | | | | | 80/tcp |
| None | 10386 | Web Server No 404 Error Code Check | | | | | 443/tcp |
| None | 10785 | Microsoft Windows SMB NativeLanManager R | | | | | 445/tcp |
| None | 10863 | SSL Certificate Information | | | | | 443/tcp |
| None | 10863 | SSL Certificate Information | | | | | 5001/tcp |
| None | 10881 | SSH Protocol Versions Supported | | | | | 2121/tcp |
| None | 10881 | SSH Protocol Versions Supported | | | | | 2323/tcp |
| None | 10884 | Network Time Protocol (NTP) Server Detec | | | | | 123/udp |
| None | 11011 | Microsoft Windows SMB Service Detection | | | | | 139/tcp |