**TLP:CLEAR**
**Szabadon terjeszthető!**

# Tájékoztatás,

# a regreSSHion sérülékenységről

(2024. július 03.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki **glibc alapú Linux rendszereket érintő, OpenSSH (regreSSHion) sérülékenységgel kapcsolatban**, annak súlyossága és kihasználhatósága miatt.

A **CVE-2024-6387, regreSSHion** néven azonosított, **8.1 pontszámú (CVSS3.1), magas kockázati besorolású** sebezhetőség – amely egy jelkezelő versenyfeltétel az OpenSSH szerverében (sshd) – lehetővé teszi a hitelesítés nélküli távoli kódfuttatást **(RCE)** root felhasználóként, a glibc-alapú Linux rendszereken.

A sebezhetőség a 2006-ban bejelentett, és már javított **CVE-2006-5051** sebezhetőség **regressziója**. Ebben a kontextusban ez azt jelenti, hogy egy egyszer már kijavított hiba egy későbbi szoftverkiadásban újra megjelenik, jellemzően olyan változtatások vagy frissítések miatt, amelyek véletlenül újra bevezetik a hibát. Ez a **regresszió** 2020 októberében került bevezetésre (OpenSSH 8.5p1).

A sebezhetőség kihasználása a rendszer teljes kompromittálódásához vezethet, ahol a támadó tetszőleges kódot futtathat a legmagasabb jogosultságokkal, ami a rendszer teljes átvételét, rosszindulatú programok telepítését, adatmanipulációt és tartós hozzáférést biztosító backdoor-ok létrehozását eredményezheti. Megkönnyítheti a hálózati terjedést, lehetővé téve a támadók számára, hogy a kompromittált rendszert kiindulópontként használják a szervezeten belüli más sebezhető rendszerek kihasználására (lateral movement).

**Az érintett OpenSSH verziók listája:**

- Az OpenSSH 4.4p1-ig terjedő verziói, valamint a glibc-Linuxon futó 8.5p1 és 9.7p1 közötti verziók sebezhetőek.
- Az OpenBSD alapú szerverek nem érintettek, mivel az OpenBSD 2001-ben kifejlesztett egy olyan biztonságos mechanizmust, amely megakadályozza ezt a sebezhetőséget.

**Az NBSZ NKI a Linux disztribúciók biztonsági közleményeiben szereplő javítások alkalmazását, az sshd 9.8-as verzióra való haladéktalan frissítését javasolja.**

Amennyiben a frissítések nem alkalmazhatóak azonnal, enyhítő intézkedésként a **LoginGraceTime** paraméter letiltása védelmet nyújthat a távoli kódvégrehajtási támadás ellen. Az **sshd kiszolgáló azonban továbbra is sebezhető a szolgáltatás megtagadásával szemben (DoS), mivel egy támadó továbbra is kimerítheti az összes kapcsolatot.**

1) Root felhasználóként nyissa meg a **(/etc/ssh/sshd_config)** állományt!

2) Adja hozzá vagy szerkessze a paraméterkonfigurációt **(LoginGraceTime 0)**!

3) Mentse és zárja be a fájlt!

4) Indítsa újra az sshd daemont **(systemctl restart sshd.service)**!

**Hivatkozások:**


- **https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server**
- **https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt**
- **https://access.redhat.com/security/cve/cve-2024-6387**
- **https://security-tracker.debian.org/tracker/CVE-2024-6387**
- **https://ubuntu.com/security/CVE-2024-6387**


**Nemzetbiztonsági Szakszolgálat**
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833