TLP:CLEAR
Szabadon terjeszthető!

Riasztás a Linux rendszereket érintő Dirty Frag sérülékenységről

Tisztelt Ügyfelünk!

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** riasztást ad ki a **Dirty Frag** néven ismert, **Linux rendszereket érintő, magas kockázatú kernel sebezhetőségről**.

A Linux kernelt érintő két helyi jogosultságkiterjesztést lehetővé tevő sebezhetőség közül csak az egyik kapott azonosítószámot (CVE-2026-43284 / EUVD-2026-28535), míg a másik jelenleg még besorolás alatt áll.

- A **CVE-2026-43284 / EUVD-2026-28535** sebezhetőség az ESP (Encapsulating Security Protocol) támogatásához kapcsolódik, amely az IPsec (Internet Protocol Security) protokoll része, és széles körben alkalmazzák VPN-kapcsolatok esetén.
- Az azonosító nélküli sebezhetőség az RxRPC protokollt érinti, amelyet például az AFS (Andrew File System) elosztott fájlrendszer használ.

A sérülékenységek számos ismert Linux disztribúciót érintenek, amelyek 2017 után kiadott kernelverziót használnak.

Hatás

Olyan rendszereken, ahol nem futnak konténeres munkaterhelések, a sérülékenység lehetővé teszi egy helyi felhasználó számára a jogosultságok root szintre történő kiterjesztését.

Konténeres környezetekben – különösen, ahol tetszőleges harmadik féltől származó konténeres alkalmazások futtatása engedélyezett – a sérülékenység nemcsak helyi jogosultságkiterjesztésre, hanem potenciálisan konténerszökésre (container escape) is felhasználható. Jelenleg azonban ilyen támadási forgatókönyvre még nem publikáltak demonstrációs célú PoC (proof of concept) exploitot.

A publikálás időpontjában a sérülékenységekhez még nem érhető el javítás vagy biztonsági frissítés, ezért javasolt az alábbi mitigációs lépések végrehajtása. A mitigáció az IPsec ESP és az RxRPC működéséhez szükséges kernelmodulok letiltásával csökkenti a kockázatot. A bemutatott mitigációs lépések Ubuntu- és Debian-alapú rendszereken közvetlenül alkalmazhatók, más Linux disztribúciók esetén kisebb módosítások válhatnak szükségessé.

A letiltás funkcionális hatással járhat az alábbi esetekben:

- IPsec-alapú VPN megoldások használata esetén (pl. StrongSwan)
- AFS (Andrew File System) vagy más RxRPC-alapú alkalmazások használata esetén

Mivel a két sérülékenység egymástól független, kizárólag az esp4/esp6 vagy kizárólag az rxrpc modulok letiltása önmagában nem elegendő.

Manuális mitigáció

A mitigáció célja az érintett kernelmodulok betöltésének megakadályozása. Ehhez három lépés szükséges:

1. A modulok jövőbeni betöltésének tiltása.
2. A jelenleg betöltött modulok eltávolítása.
3. Annak ellenőrzése, hogy a modulok valóban eltávolításra kerültek-e; sikertelenség esetén a rendszer újraindítása szükséges.

1. lépés – a modulok letiltása

Hozza létre a /etc/modprobe.d/dirty-frag.conf fájlt az alábbi tartalommal:

```
echo "install esp4 /bin/false" | sudo tee /etc/modprobe.d/dirty-frag.conf
echo "install esp6 /bin/false" | sudo tee -a /etc/modprobe.d/dirty-frag.conf
echo "install rxrpc /bin/false" | sudo tee -a /etc/modprobe.d/dirty-frag.conf
```

Ezután generálja újra az initramfs képfájlokat, hogy a modulok a rendszerindítás korai szakaszában se töltődjenek be:

```
sudo update-initramfs -u -k all
```

2. lépés – a modulok eltávolítása

Amennyiben a modulok már betöltődtek, távolítsa el őket:

```
sudo rmmod esp4 esp6 rxrpc 2>/dev/null
```

3. lépés – ellenőrzés

Ellenőrizze, hogy a modulok továbbra is aktívak-e:

```
grep -qE '^(esp4|esp6|rxrpc) ' /proc/modules && echo "Affected modules are
loaded" || echo "Affected modules are NOT loaded"
```

Amennyiben a parancs azt jelzi, hogy az érintett modulok nincsenek betöltve, további teendő nincs.

Bizonyos esetekben azonban a modulok eltávolítása nem lehetséges, mert azokat alkalmazások vagy szolgáltatások aktívan használják. Ilyenkor **a mitigáció csak rendszer-újraindítás után lép érvénybe**.

A mitigáció eltávolítása

Amint elérhetővé válik és telepítésre kerül a hivatalos kerneljavítás, a mitigáció eltávolítható.

```
sudo rm /etc/modprobe.d/dirty-frag.conf
sudo update-initramfs -u -k all
```

A legfrissebb információkért kérjük ügyfeleinket, folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

További információk

https://www.wiz.io/blog/dirty-frag-linux-kernel-local-privilege-escalation-via-esp-and-rxrpc

https://ubuntu.com/blog/dirty-frag-linux-vulnerability-fixes-available

https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2026-43284

https://nvd.nist.gov/vuln/detail/CVE-2026-43284

https://euvd.enisa.europa.eu/vulnerability/CVE-2026-43284

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