

## Riasztás a Linux rendszereket érintő Copy Fail sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a Copy Fail néven ismert, Linux rendszereket érintő, magas kockázatú kernel sebezhetőségről. A [CVE-2026-31431](#) és [EUVD-2026-24639](#) azonosítón nyomon követett hiba a Linux kernel kriptográfiai alrendszeréhez kapcsolódik. A sérülékenység CVSS v3.1 szerinti pontszáma 7.8, besorolása magas.

A hiba sikeres kihasználása esetén egy **alacsony jogosultságú helyi felhasználó vagy folyamat root jogosultságot szerezhet** az érintett Linux rendszeren. A sérülékenység önmagában nem távoli belépési hiba, azonban különösen kockázatos olyan környezetekben, ahol a támadó már képes kódot futtatni.

A sérülékenység a Linux kernel `algif_aead` komponensében korábban bevezetett in-place működéshez kapcsolódik. A javítás ezt a **működést visszavonja**, és biztonságosabb out-of-place feldolgozásra tér vissza. A hiba kihasználása a page cache módosításán keresztül `setuid` binárisok, például a `/usr/bin/su` működésének befolyásolását teheti lehetővé. Emiatt a lemezen található **fájl változatlan maradhat**, miközben a memóriában lévő példány viselkedése módosul, így a **hagyományos fájlintegritás-ellenőrzés önmagában nem feltétlenül elegendő**.

A sérülékenységhez nyilvános Proof-of-Concept is elérhető, ezért az érintett rendszerek soron kívüli ellenőrzése és javítása indokolt.

Érintettek lehetnek a **4.14-től kezdődő**, a javítást még nem tartalmazó Linux kernelverziók. Az érintettség pontos megállapításához minden esetben **a használt disztribúció biztonsági közleményeit**, a telepített **kernelcsomag verzióját**, valamint a **ténylegesen futó kernelverziót** szükséges ellenőrizni.

A kernelcsomag frissítése után **a rendszer újraindítása szükséges**, mert a javított kernel csak ezt követően válik aktívvá.

Amennyiben a rendszer érintett vagy az érintettség nem zárható ki, **javasolt a disztribúció által kiadott javított kernelcsomag soron kívüli telepítése**. Debian és Ubuntu rendszereken ez jellemzően az `apt`, RHEL-alapú rendszereken a `dnf`, SUSE rendszereken pedig a `zypper` csomagkezelővel végezhető el. A pontos javított csomagverziót minden esetben **a disztribúció hivatalos biztonsági közleménye alapján kell ellenőrizni**.

Amennyiben a kernel frissítése nem hajtható végre azonnal, **átmeneti kockázatcsökkentő lépésként javasolt az `algif_aead` modul tiltása**.

Konténeres környezetekben javasolt a **host kernel soron kívüli frissítése**, a **privilegizált konténerek**

**TLP: CLEAR**

**Szabadon terjeszthető!**

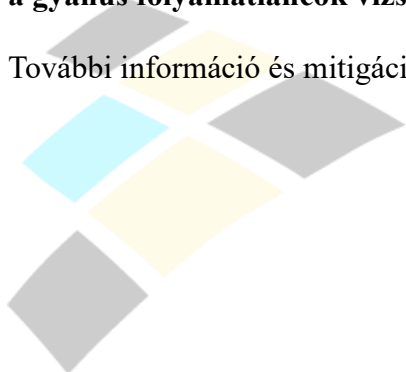
kerülése, a felesleges Linux capability-k eltávolítása, valamint seccomp profilok használata. Kubernetes esetén legalább a RuntimeDefault seccomp profil és az allowPrivilegeEscalation: false beállítás alkalmazása javasolt. Magas kockázatú vagy nem megbízható kódot futtató környezetekben érdemes külön ellenőrizni, hogy az alkalmazott seccomp profil korlátozza-e az AF\_ALG socketek létrehozását.

CI/CD rendszereknél célszerű a self-hosted runner gépeket soron kívül frissíteni, ahol lehet ephemeral runner-öket használni, korlátozni a publikus forkokból indított jobokat, valamint a build során elérhető hitelesítési adatokat, tokeneket és cloud jogosultságokat a szükséges minimumra csökkenteni.

Az érintett rendszerek utólagos vizsgálata is indokolt, különösen olyan környezetekben, ahol nem megbízható felhasználói vagy automatizált kód futott. Az ellenőrzés során érdemes vizsgálni az AF\_ALG használatára, setuid binárisok szokatlan futtatására, jogosultságkiterjesztésre, CI/CD runneren megjelenő interaktív shellre, konténerből indított gyanús hostsintű műveletekre, illetve rövid életű exploítkód futtatására utaló eseményeket.

A hiba jellege miatt fontos hangsúlyozni, hogy a fájlrendszer-alapú integritásellenőrzés önmagában nem feltétlenül elegendő. A támadás a page cache-t is érintheti, ezért központi naplógyűjtés, EDR telemetria és a gyanús folyamatláncok vizsgálata kiemelten javasolt.

További információ és mitigációs javaslatok a [Copy Fail](#) hivatalos oldalán.



NEMZETI  
KIBERBIZTONSÁGI  
INTÉZET

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

**TLP: CLEAR**