Vulnerabilități „Copy Fail” în distribuții Linux

Vulnerabilitate critică identificată în Kernel Linux
CVE-2026-31431

CVE / ID	Condiția pentru exploatare	Descriere succintă	CVSS	Tip vulnerabilitate	Mod de exploatare
CVE-2026-31431 Copy Fail	Acces local ca utilizator neprivilegiat	Logic bug în subsistemul criptografic al kernel-ului Linux. Operația in-place în algif_aead.c permite scrierea controlată de 4 bytes în page cache-ul oricărui fișier citibil, inclusiv binare setuid. Un script de 732 bytes obține root.	**Critic**	LPE / Page Cache Corruption	Local, fără privilegii, determinist

Câmp	Detalii
Cauza principală	Optimizare in-place introdusă în 2017 (commit 72548b093ee3) în algif_aead.c: paginile din page cache ale unui fișier ajung în scatterlist-ul cu scriere prin sg_chain(). authencesn scrie 4 bytes scratch la dst[assoclen+cryptlen], dincolo de buffer-ul legitim.
Triggerul	authencesn (wrapper AEAD pentru IPsec ESN) scrie seqno_lo la o adresă din afara bufferului de ieșire. scatterwalk traversează în paginile page cache și scrie direct în copia kernel a fișierului țintă.
Metode de exploatare	Socket AF_ALG + splice() + sendmsg()/recvmsg(). Script Python 732 bytes, bibliotecă standard. Target implicit: /usr/bin/su (binar setuid-root).
Versiuni afectate	Toate kernel-urile Linux expediate din 2017 (linii 6.12, 6.17, 6.18 confirmate). Ubuntu 24.04, Amazon Linux 2023, RHEL 10.1, SUSE 16.
Consecințe	Acces root local. Fișierul pe disc rămâne intact (invizibil pentru checksums). Traversare granițe containere → escape Kubernetes (Partea 2).

Vulnerabilități „Copy Fail” în distribuții Linux

Descriere

În kernel-ul Linux a fost identificată o vulnerabilitate logică critică în subsistemul criptografic AF_ALG, desemnată CVE-2026-31431 (Copy Fail). Aceasta permite unui utilizator local neprivilegiat să efectueze o scriere controlată de 4 bytes în page cache-ul oricărui fișier citibil, fără condiții de cursă, reîncercări sau ferestre de timing. Un script Python de 732 bytes obține acces root pe toate distribuțiile Linux majore expediate din 2017.

Sunt afectate Ubuntu 24.04 LTS, Amazon Linux 2023, RHEL 10.1 și SUSE 16, testate pe kernel-uri din liniile 6.12, 6.17 și 6.18. Vulnerabilitatea a existat în mod nedetectat timp de aproximativ 9 ani.

Descrierea tehnică a lanțului de exploatare

Cauza principală — sg_chain și page cache în scatterlist-ul cu scriere

AF_ALG este un tip de socket care expune subsistemul criptografic kernel spațiului utilizator neprivilegiat. Primitiva splice() transferă pagini din page cache prin referință, fără copiere. Când un utilizator conectează un fișier printr-un pipe în AF_ALG, scatterlist-ul de intrare conține referințe directe la paginile kernel ale acelui fișier. Optimizarea in-place din 2017 a setat req->src = req->dst, conectând aceste pagini prin sg_chain() în scatterlist-ul cu scriere.

Triggerul — scrierea scratch a authencesn

authencesn (wrapper AEAD pentru IPsec cu Extended Sequence Numbers) folosește bufferul de destinație ca spațiu scratch pentru rearanjarea octeților ESN. Al treilea apel scatterwalk_map_and_copy scrie 4 bytes la dst[assoclen + cryptlen] — dincolo de tag-ul AEAD, în paginile page cache ale fișierului țintă. Niciun alt algoritm AEAD standard nu face acest lucru.

Etapele lanțului de atac

1. Configurare socket: deschidere AF_ALG, bind la authencesn(hmac(sha256),cbc(aes)), fără privilegii.
2. Construirea scrierii: pentru fiecare chunk de 4 bytes din payload, se construiește o pereche sendmsg() + splice(). Octeți 4-7 din AAD (seqno_lo) = valoarea de scris. Parametrii AEAD determină offset-ul exact în .text-ul binarului țintă.
3. Declanșarea scrierii: recv() pornește decriptarea. authencesn scrie seqno_lo în page cache-ul /usr/bin/su. HMAC eșuează, recvmsg() returnează eroare, dar scrierea persistă.

Execuția: execve("/usr/bin/su")

Condiții critice pentru exploatare

- Acces local ca utilizator neprivilegiat (niciun privilegiu special necesar)
- Python 3.10+ instalat (os.splice disponibil)
- AF_ALG socket activat (implicit pe toate distribuțiile majore)
- Kernel neactualizat (orice versiune expediată între 2017 și patch-ul din Aprilie 2026)
- Fișier binar setuid prezent și citibil (ex: /usr/bin/su, prezent pe toate distribuțiile testate)

Impact operațional

- Compromitere completă a sistemului — acces root local pentru orice utilizator
- Invizibilitate față de instrumente clasice de integritate: fișierul pe disc rămâne nemodificat, doar page cache-ul este corupt
- Efect imediat system-wide: page cache-ul este partajat între toate procesele; binarul corupt este vizibil instant pentru orice execuție ulterioară
- Traversare granițe containere: page cache-ul este partajat peste limitele containerelor — vector de escape Kubernetes (detalii Partea 2)

- Portabilitate totală: același script de 732 bytes funcționează pe toate distribuțiile și arhitecturile testate, fără recompilare sau offset-uri per-distribuție

Detectare și monitorizare

Nivel sistem

- Monitorizare încărcări neobișnuite ale modulului algif_aead
- Detectare apeluri splice() → AF_ALG socket din procese neprivilegiate
- Verificare integritate page cache vs. fișier disc pentru binare setuid critice
- Monitorizare execuții din /usr/bin/su, /usr/bin/passwd și alte binare setuid

Nivel rețea / sistem

- Detectare apeluri de sistem neobișnuite: socket(AF_ALG), sendmsg(), os.splice() în lanț
- Reguli SIEM pentru: creare socket tip 38 (AF_ALG) de către utilizatori cu UID > 0, urmat de splice() pe fișiere executabile

Indicatori de compromitere (IOC)

- Shell root obținut fără autentificare sudo sau su reușită în jurnale
- Proces python3 care apelează socket(38, 5, 0) urmat de splice()
- Erori de decriptare AEAD repetate din același proces neprivilegiat
- Modificare page cache detectabilă prin comparare hash în memorie vs. disc

TTPs — MITRE ATT&CK

ID Tehnică	Tehnică	Utilizare în lanțul de atac
T1068	Exploitation for Privilege Escalation	Scrierea în page cache a unui binar setuid-root → execuție ca UID 0
T1548.001	Abuse Elevation Control Mechanism: setuid	Exploatarea binarului /usr/bin/su cu bit setuid pentru escaladare la root
T1611	Escape to Host	Page cache partajat cross-container → compromiterea nodului Kubernetes
T1055	Process Injection (Page Cache)	Injectare shellcode în page cache-ul procesului țintă fără scriere pe disc
T1562.001	Impair Defenses: Disable or Modify Tools	Modificare invizibilă pentru instrumente de integritate bazate pe checksum disc
T1059.006	Command and Scripting Interpreter: Python	Exploit implementat exclusiv în Python 3.10+, fără dependințe externe

Vulnerabilități „Copy Fail” în distribuții Linux

Ghid tehnic de detectare, mitigare și actualizare

Identificarea sistemului afectat

```
lsb_release -a
uname -r
dpkg -l 'linux-image*' | grep ^ii
dpkg -l kmod
```

Verificarea stării de expunere

Confirmarea autoritativă a expunerii sau mitigării se face prin evaluarea regulilor modprobe efective. Modulul **algif_aead** poate fi blocat în mai multe locații (/etc/modprobe.d/, /lib/modprobe.d/, /usr/lib/modprobe.d/, /run/modprobe.d/); o căutare după numele fișierului nu este suficientă.

```
sudo modprobe -n -v algif_aead 2>&1
```

Interpretarea rezultatului:

Ieșire	Stare
`install /bin/false (sau echivalent)`	Mitigat: `modprobe` nu va încărca modulul
`insmod /lib/modules/.../algif_aead.ko`	Expus: modulul se va încărca la cerere
`FATAL: Module algif_aead not found`	Modulul nu este disponibil pentru kernelul curent: se verifică versiunea kernelului instalat

Pentru a identifica fișierul (sau fișierele) care conțin regula efectivă:

```
sudo grep -lrE '^[^#]*(install|blacklist|alias)[[:space:]]+(\S+[[:space:]]
+)?algif_aead([[:space:]]|$)' \
     /etc/modprobe.conf /etc/modprobe.d/ /lib/modprobe.d/ \
     /usr/lib/modprobe.d/ /run/modprobe.d/ 2>/dev/null
```

Pentru a vedea starea curentă a modulului:

```
grep -qE '^algif_aead ' /proc/modules && echo 'încărcat' || echo
'neîncărcat'
```

Mitigare prin actualizarea pachetului kmod (Ubuntu)

Actualizarea pachetului `kmod` instalează automat regula `/etc/modprobe.d/disable-algif_aead.conf` care blochează încărcarea modulului vulnerabil până la publicarea kernelului remediat.

```
sudo apt update
sudo apt install --only-upgrade kmod
sudo rmmod algif_aead 2>/dev/null
sudo update-initramfs -u
sudo systemctl reboot
```

Verificarea versiunii `kmod` instalate:

```
dpkg -l kmod
```

Versiunile minime remediate pe Ubuntu:

Versiune Ubuntu	Pachet afectat	Versiune minimă remediată kmod	Canal
Ubuntu 25.10	kmod	34.2-2ubuntu1.1	arhiva standard
Ubuntu 25.04	kmod	34.2-1ubuntu0.25.04.1	arhiva standard
Ubuntu 24.10	kmod	32+20240611-2ubuntu3.1	arhiva standard
Ubuntu 24.04 LTS	kmod	31+20240202-2ubuntu7.2	arhiva standard
Ubuntu 22.04 LTS	kmod	29-1ubuntu1.1	arhiva standard
Ubuntu 20.04 LTS	kmod	26-1ubuntu1.1	ESM (Ubuntu Pro)
Ubuntu 18.04 LTS ESM	kmod	24-1ubuntu3.8	ESM (Ubuntu Pro)
Ubuntu 16.04 ESM	kmod	22-1ubuntu5.4	ESM (Ubuntu Pro)

Pentru versiunile LTS aflate sub ESM (14.04, 16.04, 18.04, 20.04), accesul la versiunea remediată necesită activarea abonamentului Ubuntu Pro

Mitigare manuală — fără actualizarea pachetului kmod

Procedură aplicabilă pe gazde unde pachetul kmod remediat nu este accesibil (de exemplu, sistem LTS fără abonament Ubuntu Pro activ). Efectul este echivalent funcțional cu actualizarea pachetului kmod.

```
echo "install algif_aead /bin/false" | sudo tee /etc/modprobe.d/manual-
disable-algif_aead.conf
sudo rmmod algif_aead 2>/dev/null
sudo update-initramfs -u
sudo systemctl reboot
```

Validare post-reboot:

```
sudo modprobe -n -v algif_aead 2>&1
grep -qE '^algif_aead ' /proc/modules && echo 'ÎNCĂRCAT — 
investigare' || echo 'Mitigat'
```

Validarea finală

```
uname -r
dpkg -l kmod 2>/dev/null
sudo modprobe -n -v algif_aead 2>&1
grep -qE '^algif_aead ' /proc/modules && echo 'încărcat' || echo
'neîncărcat'

sudo grep -lrE '^[^#]*(install|blacklist|alias)[[:space:]]+(\S+[[:space:]]
+)?algif_aead([[:space:]]|$)' \
     /etc/modprobe.conf /etc/modprobe.d/ /lib/modprobe.d/ \
     /usr/lib/modprobe.d/ /run/modprobe.d/ 2>/dev/null

systemctl --failed
sudo journalctl -k --since '10 min ago' | grep -iE 'alg|aead'
```

Reactivarea modulului după publicarea patch-ului kernel

După instalarea kernelului remediat, modulul poate fi reactivat dacă este necesar pentru aplicații care folosesc AF_ALG (de exemplu libkcapi, validare FIPS, anumite drivere hardware crypto). Pentru a anula blocarea fără a edita fișierele instalate prin pachet (acestea se rescriu la următoarea actualizare a pachetului kmod), se creează un fișier cu prioritate mai mare în /etc/modprobe.d/:

```
sudo tee /etc/modprobe.d/00-algif_aead-reenable.conf > /dev/null <<'EOF'
# Reactivare algif_aead după patch kernel CVE-2026-31431
install algif_aead /sbin/modprobe --ignore-install algif_aead
EOF

sudo update-initramfs -u
sudo modprobe -n -v algif_aead 2>&1
sudo modprobe algif_aead
grep -qE '^algif_aead ' /proc/modules && echo 'Modul reactivat'
```

Prioritatea `/etc/modprobe.d/` față de `/lib/modprobe.d/` asigură că suprareglarea persistă chiar dacă pachetul kmod este reinstalat sau actualizat ulterior.

Surse oficiale — Ubuntu

https://ubuntu.com/blog/copy-fail-vulnerability-fixes-available
https://ubuntu.com/security/CVE-2026-31431
https://ubuntu.com/security/notices
https://bugs.launchpad.net/ubuntu/+source/linux/+bug/2150686
https://bugs.launchpad.net/ubuntu/+source/kmod/+bug/2150743

Referințe oficiale pe alte distribuții

CVE-ul este același (CVE-2026-31431), însă mecanismul de livrare a patch-ului (kernel direct vs. blocare modul vs. errata multiple) diferă pe distribuție. Administratorii consultă advisory-urile oficiale ale furnizorului.

Debian

- Debian Security Tracker: https://security-tracker.debian.org/tracker/CVE-2026-31431
- Debian Security Advisories: https://www.debian.org/security/
- Status: patch kernel disponibil în `security.debian.org` pentru Bullseye (11), Bookworm (12, DSA-6238-1) și Trixie (13, DSA-6243-1)
- Pachet sursă afectat: `linux`, `linux-6.1`

Red Hat Enterprise Linux

- Pagina CVE Red Hat: https://access.redhat.com/security/cve/CVE-2026-31431
- Portal errata RHSA: https://access.redhat.com/security/security-updates/

Vulnerabilități „Copy Fail” în distribuții Linux

AlmaLinux

- Portal errata AlmaLinux: https://errata.almalinux.org/
- Căutare în portal după string `CVE-2026-31431`

Rocky Linux

- Portal errata Rocky Linux: https://errata.rockylinux.org/

Oracle Linux

- Pagina CVE Oracle Linux: https://linux.oracle.com/cve/CVE-2026-31431.html
- Portal errata ELSA: https://linux.oracle.com/errata.html
- Referințe ELSA aplicabile: ELSA-2026-13565 / 13566 / 13577 (kernel RHCK), ELSA-2026-50253 / 50254 / 50255 / 50260 / 50261 / 50262 (kernel-uek)

SUSE Linux Enterprise / openSUSE

- Pagina CVE SUSE: https://www.suse.com/security/cve/CVE-2026-31431/
- Portal SUSE-SU errata: https://www.suse.com/support/update/

Amazon Linux

- Amazon Linux 2: https://alas.aws.amazon.com/AL2/
- Amazon Linux 2023: https://alas.aws.amazon.com/AL2023/
- Amazon Linux 2026: https://alas.aws.amazon.com/

Arch Linux

- Pagina advisory: https://security.archlinux.org/CVE-2026-31431
- Status: rezolvat prin actualizare standard `pacman -Syu` la kernelul curent

CentOS Stream

- CentOS Stream 8: end-of-life din 2024-05-31; migrare către AlmaLinux 8, Rocky Linux 8 sau RHEL 8
- CentOS Stream 9: tracker prin pagina CVE Red Hat — https://access.redhat.com/security/cve/CVE-2026-31431

Referințe tehnice și de tracking globale

- NVD: https://nvd.nist.gov/vuln/detail/CVE-2026-31431
- MITRE CVE Record: https://www.cve.org/CVERecord?id=CVE-2026-31431
- CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Commit upstream de remediere (kernel.org): https://git.kernel.org/linus/a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5
- Discuție oss-security (aprilie–mai 2026): https://www.openwall.com/lists/oss-security/
- Publicație tehnică PoC și write-up: https://copy.fail