SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

RAPORT TEHNIC DE SECURITATE

Vulnerabilitate în implementarea TCP IPv4 din Linux

CVE-2026-98432

Utilizarea memoriei după eliberare
Risc de compromitere a nucleului de la distanță

Ubuntu și Red Hat Enterprise Linux
Versiuni afectate și măsuri de remediere

1 Sumar executiv și fișa vulnerabilității

Se recomandă inventarierea urgentă a nucleelor Linux și prioritizarea serverelor care acceptă conexiuni IPv4 din rețele de neîncredere. Remedierea constă în activarea unui nucleu corectat și suportat de distribuție. Pentru sistemele fără pachet disponibil se reduc căile de acces și se urmărește zilnic starea furnizorului, cu responsabil și termen de reevaluare.

CVE-2026-98432 descrie o condiție de concurență în procesarea TCP IPv4 care poate permite utilizarea unei structuri de opțiuni IP după eliberarea memoriei. Articolul Cyberkendra din 29 octombrie 2026 evidențiază riscul pentru Ubuntu și RHEL. O demonstrație de cercetare anunțată de Anthropic descrie executarea comenzilor ca root prin intermediul unui serviciu MPTCP.

Câmp	Date tehnice
Identificator și autoritate	CVE-2026-98432; autoritate CNA Linux; publicare la 15 octombrie 2026.
Componentă	Nucleul Linux, TCP IPv4; net/ipv4/af_inet.c și net/ipv4/tcp_ipv4.c.
Tipul defectului	Use-after-free, asociat unei condiții de concurență. Red Hat indică CWE-825, Expired Pointer Dereference.
Acces necesar	Acces de rețea la o cale TCP afectată, fără credențiale și fără interacțiunea utilizatorului în scenariul CNA.
Severitate CNA	CVSS v3.1 9,8 Critic; impact ridicat asupra confidențialității, integrității și disponibilității.
Exploatare	Demonstrație de cercetare publicată; nu este echivalentă cu o confirmare a atacurilor reale.
Decizie operațională	Verificarea pachetului complet, a expunerii și a nucleului efectiv pornit; controale temporare până la remediere.

2 Cauza tehnică și corecția din nucleu

Durata de viață a opțiunilor IPv4

La crearea unui socket TCP copil, tcp_v4_syn_recv_sock() transferă pointerul ireq_opt în inet_opt fără a copia structura. În paralel, un alt procesor poate încă utiliza opțiunile pentru a construi răspunsul SYNACK la un SYN retransmis. Distrugerea copilului eliberează memoria înainte ca cititorul să termine, ceea ce produce utilizarea memoriei după eliberare.

Defectul privește sincronizarea dintre citire și eliberare. Conținutul unei zone eliberate se poate modifica înainte de reutilizarea pointerului. CNA descrie posibilitatea divulgării de memorie, a coruperii memoriei și a căderii nucleului.

Cele două căi descrise de dezvoltatori

Cale	Situația relevantă	Consecință pentru evaluare
Conexiune TCP IPv4	Prelucrarea concurentă a unui SYN retransmis și eliberarea opțiunilor socketului copil.	Valoarea tcp_migrate_req=0 nu exclude această cale.
Migrarea cererii	O cerere și clona sa partajează opțiunile; migrare prin tcp_migrate_req=1 sau program BPF de tip SELECT_OR_MIGRATE. [4]	Se examinează configurația SO_REUSEPORT și politica BPF aplicabilă.

Eliberarea după perioada de grație RCU

Corecția înlocuiește eliberarea imediată cu kfree_rcu() în inet_sock_destruct() și tcp_v4_reqsk_destructor(). RCU, Read Copy Update, permite amânarea eliberării până când cititorii anteriori au încheiat accesul. Modificarea aliniază distrugerea obiectului cu protecția deja utilizată de cititori.

```
/* Principiul corecției în inet_sock_destruct() */
/* Înainte */
kfree(rcu_dereference_protected(inet->inet_opt, 1));
/* După corecție */
kfree_rcu(rcu_dereference_protected(inet->inet_opt, 1), rcu);
```

Commitul principal este e3f33b0a1d89d738e2b913dab519226eaf76e15b. Fragmentul ilustrează remedierea; instalarea unui pachet suportat rămâne calea recomandată pentru sisteme de producție.

Limitele concluziilor despre IPv6

Dezvoltatorii precizează că prima problemă nu afectează calea IPv6, unde opțiunile sunt copiate. Aceeași descriere menționează separat o problemă de migrare asociată CALIPSO, destinată altei corecții. Afirmația nu trebuie extinsă la securitatea tuturor căilor IPv6.

3 Severitate și starea exploatării

Scoruri CVSS atribuite de surse diferite

Scorurile se păstrează împreună cu autoritatea și vectorul lor. Diferența principală dintre CNA și evaluările de 8,1 este complexitatea atacului, AC:L față de AC:H.

Sursă	CVSS v3.1	Complexitate	C / I / A
Linux CNA	9,8 Critic	Scăzută	Ridicat / Ridicat / Ridicat
Red Hat tabel CVSS	8,1 Ridicat	Ridicată	Ridicat / Ridicat / Ridicat
Oracle Linux	8,1 Ridicat	Ridicată	Ridicat / Ridicat / Ridicat
Amazon Linux	8,1 Ridicat	Ridicată	Ridicat / Ridicat / Ridicat
SUSE	8,1 Ridicat	Ridicată	Ridicat / Ridicat / Ridicat

4 Ramuri Linux și versiuni remediate upstream

Înregistrarea Linux CNA, actualizată la 30 octombrie 2026, enumeră versiunile de mai jos ca remediate pentru acest CVE. Tabelul se aplică ramurilor upstream; pachetele distribuțiilor au propriile revizii și propriile corecții preluate înapoi.

Ramură	Prima versiune remediată	Commit abreviat
5.10	5.10.272	b3b027ef0cd3
5.15	5.15.223	95a8c8fa9f27
6.1	6.1.190	89b5b1eb7d63
6.6	6.6.159	742f73df544e
6.12	6.12.113	11a03ce3c4a6
6.18	6.18.56	a47406c769f7
7.2	7.2.10	26d4c36d318c
Principală	7.3	e3f33b0a1d89

Introducerea defectului

Echipa Linux indică introducerea problemei în seria 4.4, prin commitul 079096f103fa. Această referință este utilă pentru analiza arborilor de surse; nu justifică alegerea unui nucleu vechi, fără suport, doar pentru a evita acest CVE.

Ramura principală și versiunile candidate

Anunțul inițial menționează 7.3-rc7 pentru commitul principal, iar înregistrarea CNA curentă indică 7.3 ca versiune remediată. O versiune release candidate nu reprezintă implicit o țintă potrivită pentru producție.

Interpretarea corectă a numerelor de versiune

Un pachet cu bază 5.14 sau 6.8 poate primi corecția fără a adopta numărul upstream din tabel. Invers, simpla instalare a unui pachet nou nu confirmă că sistemul l-a pornit. Evaluarea trebuie să lege avizul furnizorului, versiunea completă a pachetului și nucleul efectiv activ.
Pentru arbori întreținuți local se verifică includerea corecției și a dependențelor sale pe ramura exactă. Un hash diferit poate reprezenta un backport valid. Compararea exclusivă a hashului principal sau a șirului uname -r este insuficientă. Versiunile enumerate remediază vulnerabilitatea analizată. Ținta de actualizare se verifică și față de celelalte avize aplicabile, compatibilitatea driverelor și ciclul de suport.

5 Starea Ubuntu și Red Hat Enterprise Linux

Ubuntu

Canonical atribuie prioritate High. Pagina CVE, actualizată la 29 octombrie, păstrează pachetul linux ca vulnerabil pentru edițiile de mai jos. Versiunile aflate în lucru nu sunt prezentate ca actualizări deja disponibile.

Ediție Ubuntu	Stare pentru linux	Versiune aflată în lucru
26.10	Vulnerabil	7.3.0-10.10
26.04 LTS	Vulnerabil	7.0.0-43.43
24.04 LTS	Vulnerabil	6.8.0-149.149
22.04 LTS	Vulnerabil	5.15.0-203.213
20.04 LTS	Vulnerabil	Fără versiune indicată în acest rând
18.04 LTS și 16.04 LTS	Vulnerabil	Fără versiune indicată în aceste rânduri

Pentru 22.04, linux-hwe-6.8 este vulnerabil, cu 6.8.0-149.149~22.04.1 în lucru. Variantele cloud, FIPS și real-time au rânduri distincte și necesită verificarea pachetului folosit efectiv.

Red Hat Enterprise Linux

Declarația Red Hat identifică RHEL 8, 9 și 10, inclusiv variante Real Time, Red Hat In-Vehicle OS 2 și noduri RHEL CoreOS din OpenShift 4. Corecțiile sunt descrise ca amânate pentru o actualizare viitoare, fără termen publicat. RHEL 7 este declarat neafectat.
Starea Fix deferred nu garantează o corecție. Red Hat nu indică o măsură temporară care să îndeplinească criteriile sale de mitigare. Pentru RHEL 6, mențiunea Out of support scope nu înseamnă neafectat.

Gestionarea sistemelor fără pachet disponibil

Administratorul confirmă ediția, canalul de suport și familia nucleului, apoi urmărește avizul pentru acel pachet. Se înregistrează expunerea rămasă, controalele aplicate, responsabilul și următoarea verificare. Înlocuirea cu un nucleu generic din altă distribuție necesită o evaluare de compatibilitate și suport.
Un sistem se marchează remediat numai pe baza unui pachet confirmat de furnizor și activat pe gazdă ori a unei corecții live cu acoperire demonstrată pentru CVE-ul și nucleul respectiv.

6 Corecții în alte distribuții Linux

Selecția de mai jos arată de ce starea trebuie evaluată pentru pachet și canal, nu numai pentru numele distribuției. Nu este o listă exhaustivă a tuturor edițiilor, arhitecturilor sau variantelor de nucleu.

Distribuție și pachet	Versiune sau aviz remediat	Observație
Debian 12 bookworm linux, security	6.1.190-1 DLA-4841-1	Pachetul de bază 6.1.176-1 apare vulnerabil.
Debian 13 trixie linux, security	6.12.113-1 DSA-6568-1	Pachetul de bază 6.12.107-1 apare vulnerabil.
Oracle Linux 7 și 8 UEK R6	ELSA-2026-500397	Exemplu OL8: 5.4.17-2136.360.3.1.el8uek.
Oracle Linux 8 și 9 UEK R7	ELSA-2026-500398	Exemplu OL9: 5.15.0-325.221.6.4.el9uek.
Oracle Linux 9 și 10 UEK R8	ELSA-2026-500399	Exemplu OL9: 6.12.0-207.111.5.4.el9uek.
SLES 16.0 kernel-default	6.12.0-160000.40.1	Stare Released; pachetul trebuie activat pe gazdă.
SUSE Linux Micro 6.2 kernel-default	6.12.0-160000.40.1	Stare Released; nu se extinde automat la alte ediții.
Amazon Linux 2023 kernel6.18	ALAS2023-2026-3251	Publicat la 24 octombrie; stare Fixed pentru acest pachet.

Variante care rămân de urmărit

SUSE indică kernel-default din SLES 15 SP7 ca afectat, cu kernel-source în lucru. Amazon păstrează pachetul kernel implicit din AL2023 și variantele AL2 enumerate în pagina CVE ca Pending Fix.

Aplicabilitatea avizelor Oracle

Cele trei avize UEK sunt publicate la 16 octombrie. Alegerea se face după UEK R6, R7 sau R8, ediție și arhitectură. Starea UEK nu confirmă starea unui Red Hat Compatible Kernel de pe aceeași instalare. Exemplele din tabel nu reprezintă versiuni interșanjabile între produse.

7 Inventariere și verificări neintruzive

Inventarul trebuie să includă gazdele fizice, mașinile virtuale, nodurile clusterelor și echipamentele Linux administrate ca appliance. Pentru produse integrate se solicită confirmarea furnizorului produsului privind nucleul inclus și calea suportată de actualizare.

Câmp de inventar	Dovadă necesară
Identificare și rol	Identificator intern, serviciu, responsabil, importanță și dependențe.
Nucleu și pachet	Versiune pornită, distribuție, revizie completă, arhitectură, canal și aviz aplicabil.
Accesibilitate IPv4	Interfețe, porturi, surse permise și punctul unde este procesată conexiunea TCP.
MPTCP și migrare	Listeneri MPTCP, namespace de rețea, sysctl și politica BPF relevantă.
Remediere și evidențe	Pachet țintă, data disponibilității, fereastră de intervenție și rezultat după pornire.

Identificarea versiunii și a socketurilor

```
uname -r
cat /etc/os-release
ss -lntp
ss -M -l -n -p
sysctl net.mptcp.enabled net.ipv4.tcp_migrate_req
```

ss -M selectează socketurile MPTCP. Citirea proceselor și a tuturor namespace-urilor poate necesita privilegii administrative. Un iproute2 vechi poate să nu recunoască opțiunea. Eroarea comenzii sau o listă goală nu justifică automat marcarea gazdei ca neafectată.

Pachete din familiile Debian și RPM

```
# Debian / Ubuntu
dpkg-query -W -f='${Package} ${Version} ${db:Status-Abbrev}\n' 'linux-image-*'
# RHEL și derivate, după familia instalată
rpm -q kernel kernel-core kernel-rt-core kernel-uek kernel-uek-core
```

Interogările sunt exemple de citire. Se diferențiază pachetul instalat de o intrare rămasă în baza de date și se corelează rezultatul cu uname -r. Absența unui nume RPM din listă poate fi normală pentru familia folosită.

net.mptcp.enabled=1 permite crearea socketurilor MPTCP în namespace; nu dovedește existența unui listener. tcp_migrate_req are implicit valoarea 0, iar politica BPF trebuie evaluată separat.

8 Detectare și analiza evenimentelor

Se corelează telemetria de rețea cu evenimentele nucleului și cu activitatea de pe gazdă. Semnalele de mai jos sunt ipoteze de investigație; nu sunt semnături exclusive pentru acest CVE.

Semnal	Date de corelat	Limită
Kernel oops sau panic	Ora, versiunea, stack trace, rebooturi și modificări recente.	Mai multe defecte pot produce același efect.
Mesaje de memorie invalidă	use-after-free, KASAN și funcții din calea IPv4/TCP.	KASAN nu este activ pe toate nucleele de producție.
Trafic IPv4 cu opțiuni	Antetul IP, retransmisii, serviciu destinație și fereastra incidentului.	Traficul poate fi legitim; fluxurile agregate pot omite opțiunile IP.
Activitate neașteptată ca root	Procese, servicii, persistență, conexiuni și schimbări de fișiere.	Necesită triere ca posibil incident, fără atribuirea automată acestui CVE.
Goluri în telemetrie	Retenție, ceasuri, pierderi de pachete și accesul la jurnale.	Lipsa datelor nu exclude o tentativă sau o compromitere.

Căutare orientativă în jurnalul nucleului

```
journalctl _TRANSPORT=kernel --since '2026-10-15 00:00:00' --no-pager |
  grep -Ei -e 'KASAN|use-after-free' \
    -e 'ip_options_build|tcp_v4|inet_sock_destruct'
```

Filtrul folosește câmpul jurnalului pentru mesajele nucleului și poate acoperi porniri istorice, în limita retenției și a permisiunilor. Data se adaptează ferestrei de investigație; ea nu reprezintă începutul cert al expunerii.

Interpretarea absenței erorilor

Anthropic afirmă că pierderea cursei în demonstrația sa poate eșua doar conexiunea respectivă, fără prăbușirea serverului. Prin urmare, absența unui kernel panic nu este un criteriu suficient pentru excluderea tentativelor.
Opțiunile IPv4 Record Route și IP Timestamp menționate de CNA sunt diferite de opțiunea TCP Timestamp. O regulă construită doar pe setarea tcp_timestamps sau pe retransmisii obișnuite poate produce concluzii greșite.
Sursele folosite nu furnizează o listă verificată de adrese IP, domenii sau hashuri malițioase specifice acestui CVE. Indicatorii locali se păstrează cu sursa, ora și gradul de încredere.

9 Remediere și reducerea expunerii

Actualizarea nucleului

Echipa de administrare confirmă pachetul remediat pentru familia instalată, inclusiv arhitectura și canalul de suport. Se verifică semnătura pachetului, compatibilitatea modulelor, accesul la consola de recuperare și procedura de revenire. Actualizarea se testează pe un nod reprezentativ prin verificări funcționale ale serviciilor.

După instalare se planifică repornirea, se confirmă nucleul activ și se păstrează dovada avizului care acoperă CVE-2026-98432. În clustere, operația se face controlat pentru fiecare nod, cu verificarea capacității și a redundanței. Un nod de rezervă rămas vulnerabil menține o cale de expunere.

O soluție livepatch este acceptată ca remediere doar dacă furnizorul confirmă acoperirea exactă a CVE-ului pentru nucleul pornit și aplicarea este verificată. Existența unui abonament sau a agentului livepatch nu constituie această dovadă.

Controale temporare recomandate local

- Restrângerea accesului IPv4 la serviciile afectate prin controale de rețea și liste de surse permise, unde funcția serviciului permite acest lucru.
- Oprirea serviciilor TCP inutile și revizuirea listenerilor MPTCP identificați, după evaluarea impactului asupra aplicațiilor.
- Separarea serviciilor publice de funcțiile de administrare și de resursele sensibile; verificarea traficului permis și din rețeaua internă.
- Testarea oricărei filtrări a opțiunilor IPv4 pe echipamentul care o aplică și validarea traseelor alternative înainte de a conta pe ea.

Acestea sunt recomandări de reducere a riscului. Nu reprezintă o corecție a defectului sau o mitigare completă certificată pentru fiecare produs. Pentru controalele implementate se măsoară accesibilitatea rămasă și impactul funcțional.

Măsuri care nu dovedesc remedierea

Dezactivarea MPTCP nu este demonstrată ca soluție completă pentru defectul TCP IPv4. Valoarea tcp_migrate_req=0 nu elimină prima cale de concurență. Autentificarea aplicației, WAF-ul sau un control de rată nu se consideră suficiente fără dovada că blochează calea anterioară autentificării.

Dacă nu există încă o actualizare suportată, responsabilul de risc aprobă perioada de expunere reziduală conform procedurii organizației. Verificarea furnizorului continuă până la activarea corecției.

10 Surse și referințe

Surse publice consultate la 30 octombrie 2026. Stările de pachet și scorurile sunt informații care se pot modifica; decizia de actualizare se verifică din nou la momentul intervenției.

Cyberkendra Articolul de referință Publicat la 29 octombrie 2026.

Linux CNA Înregistrarea CVE-2026-98432 Metadate, CVSS și ramuri; actualizare 30 octombrie.

Linux CVE Team Anunțul vulnerabilității Descriere tehnică și referințe; 15 octombrie 2026.

Linux Commitul principal al corecției ipv4: free inet_opt and ireq_opt after an RCU grace period.

Anthropic Discovering vulnerabilities with Claude Secțiunea 5, demonstrația Linux; 27 octombrie 2026.

Red Hat CVE-2026-98432 Produse, declarație, mitigare și tabel CVSS.

Canonical Ubuntu CVE-2026-98432 Prioritate și stări pe pachet; actualizare 29 octombrie.

Debian Security Tracker CVE-2026-98432 Versiuni linux și avizele Debian.

Oracle Linux CVE-2026-98432 Scor și asocierea produselor cu avizele UEK.

Amazon Linux CVE-2026-98432 Scor și stări pe familii de pachete.

SUSE CVE-2026-98432 Pachete remediate și stări pe produse.

Linux Kernel Multipath TCP Comportamentul și utilizarea MPTCP de aplicații.

Linux Kernel MPTCP sysctl Semnificația net.mptcp.enabled.

Linux Kernel IP sysctl tcp_migrate_req și tcp_timestamps.

iproute2 Manualul ss Inventarierea socketurilor și opțiunea MPTCP.

CISA Known Exploited Vulnerabilities Copia fluxului publicată la 29 octombrie 2026, 19:09 UTC.

Debian Manualul dpkg-query Interogarea versiunii și a stării pachetelor.

RPM Manualul rpm Interogarea pachetelor instalate.

systemd Manualul journalctl Filtrarea jurnalului și intervalele de timp.

Oracle ELSA-2026-500397 UEK R6; 16 octombrie 2026.

Oracle ELSA-2026-500398 UEK R7; 16 octombrie 2026.

Oracle ELSA-2026-500399 UEK R8; 16 octombrie 2026.

Amazon ALAS2023-2026-3251 kernel6.18; publicat la 24 octombrie 2026.