SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

RAPORT TEHNIC DE SECURITATE

Cisco Secure Firewall
Indisponibilizarea
serviciului VPN SSL

CVE-2026-76418

Repornire de la distanță fără autentificare
Exploatare activă confirmată de Cisco

1 Sumar executiv și fișa vulnerabilității

Se recomandă evaluarea urgentă a echipamentelor Cisco ASA și FTD care oferă acces VPN SSL, urmată de instalarea versiunii remediate compatibile cu platforma. Prioritatea revine interfețelor accesibile din internet și echipamentelor care susțin servicii critice. Evaluarea trebuie să includă grupurile de conexiune și autentificarea secundară, nu numai versiunea afișată.

Articolul din 28 octombrie 2026 privește CVE-2026-76418. Cisco confirmă exploatarea activă în octombrie. Vulnerabilitatea permite unei cereri special construite să provoace repornirea dispozitivului înaintea unei autentificări VPN reușite. Impactul declarat este indisponibilizarea serviciului, de tip denial of service, DoS.

Câmp	Evaluare tehnică
Identificatori	CVE-2026-76418; aviz cisco-sa-asaftd-tunnel-dos-s6mgkb75; defect Cisco CSCwx26625.
Produse	Cisco Secure Firewall Adaptive Security Appliance Software, ASA, și Secure Firewall Threat Defense Software, FTD.
Serviciu	Remote Access SSL VPN; calea afectată depinde de configurarea autentificării secundare pe tunnel group.
Acces necesar	Atacator la distanță, fără cont sau autentificare VPN reușită și fără interacțiunea unui utilizator.
Severitate	8,6 Ridicat, CVSS v3.1, publicat de Cisco CNA, autoritatea de atribuire CVE.
Clasificare	CWE-690, valoare de retur neverificată care conduce la dereferențierea unui pointer NULL.
Acțiune principală	Actualizare pe fiecare nod și confirmarea versiunii efectiv pornite; măsurile temporare sunt condiționate.

2 Condiții de expunere și verificarea grupurilor

Evaluarea corelează trei elemente: software afectat, serviciu de autentificare VPN SSL accesibil și autentificare secundară în grupurile relevante. Admiterea unei conexiuni TCP sau afișarea unei pagini VPN oferă numai informații despre accesibilitate, nu confirmarea întregii configurații.

Element de verificat	Dovadă urmărită
Versiunea software	Identificarea exactă ASA sau FTD, cu revizia completă, și corelarea cu avizul Cisco.
Serviciul VPN SSL	Configurație webvpn cu enable pentru cel puțin o interfață și calea reală de acces.
Autentificarea secundară	Valoarea efectivă secondary-authentication-server-group în domeniul grupurilor stabilit mai jos.

Domeniul grupurilor care trebuie inspectate

Starea listei de grupuri	Domeniu de control conform Cisco
tunnel-group-list enable prezent	Toate grupurile de tunel, inclusiv DefaultWEBVPNGroup; verificarea nu se limitează la profilurile afișate în pagina de autentificare.
Lista lipsește sau a fost dezactivată	Se verifică DefaultWEBVPNGroup. Expunerea rămâne relevantă dacă grupul implicit utilizează autentificare secundară.

Semnificația autentificării secundare

Documentația ASA definește secondary-authentication-server-group ca grup AAA secundar asociat sesiunii în configurația cu autentificare dublă. Opțiunea se află în atributele generale ale unui tunnel group. O etichetă administrativă precum MFA sau 2FA nu înlocuiește verificarea acestei configurații specifice.

Valoarea implicită documentată este none. Apariția numelui opțiunii într-o afișare care include valorile implicite nu demonstrează activarea autentificării secundare. Se interpretează valoarea și politica efectivă.

Protecția prin autentificare a utilizatorului nu este o dovadă suficientă că procesarea vulnerabilă este inaccesibilă. În acest caz, accesul la calea afectată precede autentificarea VPN reușită. Se evaluează separat restricțiile de rețea și mecanismul de autentificare.

Produse declarate neafectate de acest CVE

Cisco enumeră Cloud-delivered Firewall, Cloud-delivered Firewall Management Center, Secure Access și Secure FMC Software. Un manager FMC neafectat poate administra dispozitive FTD care necesită remediere. Starea managerului și starea dispozitivului se înregistrează separat.

3 Versiuni remediate și alegerea țintei

Tabelele reproduc identificatorii de versiune din secțiunea First Fixed Release a avizului Cisco consultat la 29 octombrie 2026. Sunt praguri pentru acest CVE; ținta efectivă trebuie verificată și pentru compatibilitate și celelalte vulnerabilități aplicabile.

Cisco ASA

Ramură din aviz	Versiune remediată indicată
9.16 și anterioare	9.16.4.104
9.18	9.18.4.96
9.20	9.20.4.50
9.22	9.22.3.200
9.23	9.23.1.48
9.24	9.24.1.27 / 9.24.10.1

Cisco FTD

Ramură din aviz	Versiune remediată indicată
7.0 și anterioare	7.0.11
7.2	7.2.13
7.4	7.4.9
7.6	7.6.7
7.7	7.7.14
10.0	10.0.3
10.1	10.1.1

Pentru ASA 9.24 sunt enumerate două builduri remediate. Alegerea se face pentru ramura și calea de actualizare corespunzătoare; nu se presupune că ambele trebuie instalate. Versiunile și platformele neacoperite de tabel se clarifică prin Cisco Software Checker sau TAC.

4 Inventariere și colectare neintruzivă

Se includ echipamentele active, cele de rezervă și instanțele virtuale care oferă același serviciu. Inventarul se construiește din surse interne și din configurația efectiv aplicată, fără publicarea configurațiilor sau a informațiilor de autentificare.

Câmp	Informație necesară
Echipament	Model, identificator intern, rol, locație logică și responsabil.
Software	ASA sau FTD, versiune completă pornită, imagine și dovada statutului Cisco.
Acces VPN	Interfețe și căi de acces, restricții de rețea, servicii și utilizatori dependenți.
Grupuri și AAA	Starea listei, grupul implicit, grupurile relevante și autentificarea secundară efectivă.
Administrare și redundanță	FMC, FDM ori administrare ASA, noduri HA, starea sincronizării și calea de management.
Remediere	Țintă software, compatibilitate, fereastră de intervenție și dovezi de acceptare.

Exemple de comenzi ASA pentru citire

Comenzile se execută de administrator în contextul potrivit și se adaptează versiunii. Opțiunea all poate afișa și valori implicite. Rezultatele pot conține date sensibile și se păstrează în circuitul intern.

```
show version
show running-config webvpn
show running-config tunnel-group
show running-config all tunnel-group DefaultWEBVPNGroup
show failover
show vpn-sessiondb summary
```

Verificarea unei instalări FTD

Avizul indică verificarea politicii VPN aplicate din Devices > VPN > Remote Access în FMC sau din Remote Access VPN în FDM, împreună cu configurația rezultată pe dispozitiv. Se diferențiază o modificare salvată în manager de una implementată cu succes.

Pentru FTD se folosesc comenzile și interfața de diagnostic suportate de versiunea instalată. Configurațiile nu se modifică manual în afara mecanismului de administrare al produsului. Se consemnează momentul colectării, nodul și politica aplicată.

5 Detectare și corelarea evenimentelor

Detectarea urmărește disponibilitatea dispozitivului și succesiunea evenimentelor VPN. O repornire neplanificată se investighează prin corelare cu configurația și traficul disponibil; nu este, singură, o semnătură exclusivă pentru CVE-2026-76418.

Semnal	Dovezi de corelat	Limită de interpretare
Repornire sau proces căzut	Ora, uptime, motiv de reload, crashinfo, versiune și intervenții planificate.	Se exclud actualizările, alimentarea și alte defecte software.
Întreruperea sesiunilor VPN	Scăderea sesiunilor, reconectări și reclamații din aceeași fereastră.	Pierderea sesiunilor poate avea și cauze externe dispozitivului.
Acces la serviciul VPN înaintea incidentului	Sursă, interfață, profil și telemetrie de rețea disponibilă.	Cererea relevantă poate să nu apară complet în jurnal; vizibilitatea TLS contează.
Schimbare HA	Nod activ, motiv de failover, sincronizare și comportamentul partenerului.	Redundanța poate reduce întreruperea, fără să corecteze software-ul ambelor noduri.
Erori AAA sau de profil	Politica, grupul implicit și modificările de autentificare.	Lipsa unui login eșuat înregistrat nu exclude o cale anterioară autentificării.

Comenzi de sprijin pentru investigația ASA

```
show crashinfo files
show crashinfo
show failover history
show vpn-sessiondb summary
```

6 Măsuri temporare și condiții de aplicare

Cisco indică actualizarea drept remediere și descrie separat două măsuri de reducere temporară a expunerii. Alegerea se face după configurația grupului implicit, cu verificarea impactului asupra autentificării și a accesului legitim.

Condiție	Măsură descrisă de Cisco	Efect și limită
DefaultWEBVPNGroup nu utilizează autentificare secundară	În modul WebVPN: no tunnel-group-list enable.	Utilizatorii nu mai aleg profilul din listă și trebuie să cunoască profilul potrivit.
DefaultWEBVPNGroup utilizează autentificare secundară	Eliminarea atributului prin no secondary-authentication-server-group.	Reduce protecția autentificării VPN; simpla ascundere a listei nu rezolvă acest caz.

Contextul comenzii pentru autentificare

Documentația ASA situează comanda de eliminare în modul tunnel-group general-attributes. Aceasta este o descriere tehnică a măsurii temporare; nu se aplică automat tuturor grupurilor și nu se tratează ca o configurație de securitate permanentă.

Pentru un dispozitiv administrat prin FMC sau FDM se verifică metoda suportată de modificare și rezultatul implementării. Se documentează grupul, diferența de configurație, responsabilul, durata și revenirea la politica aprobată după instalarea corecției.

Validarea înaintea unei schimbări temporare

- Se confirmă starea exactă a grupului implicit și domeniul grupurilor care trebuie verificate. Eliminarea vizibilității unui profil nu demonstrează eliminarea tuturor căilor relevante.
- Se stabilește ce protecție de autentificare s-ar pierde și dacă serviciul poate fi restrâns temporar la utilizatori ori rețele justificate, fără deschiderea unei căi de acces mai puțin controlate.
- Se testează selectarea profilului și accesul legitim, se asigură administrarea de recuperare și se urmărește rezultatul pe ambele noduri, dacă există redundanță.

Controale compensatorii propuse de raport

Pot fi evaluate restricționarea surselor către serviciul VPN, retragerea temporară a unei interfețe neesențiale și folosirea unei căi de acces alternative deja aprobate. Acoperirea fiecărei măsuri se verifică pentru arhitectura existentă. Aceste controale reduc accesibilitatea sau impactul și nu modifică defectul din software.

Prioritatea rămâne instalarea versiunii corectate. O reducere temporară a autentificării se încheie prin revenirea la politica aprobată, cu verificări funcționale și de securitate.

7 Surse și limite metodologice

Analiză la 29 octombrie 2026. Tema provine din articolul SecurityOnline publicat la 28 octombrie. Condițiile de expunere, versiunile și măsurile temporare sunt preluate din avizul Cisco. Scorul, CWE și confirmarea exploatării sunt confruntate cu înregistrarea CNA.

SecurityOnline — Articolul tematic despre exploatarea serviciului VPN SSL

Cisco PSIRT — Avizul cisco sa asaftd tunnel dos s6mgkb75

Cisco CNA și CVE Program — Înregistrarea completă CVE 2026 76418

Cisco ASA Command Reference — Autentificarea secundară și grupurile AAA

Cisco ASA Command Reference — Comenzi de afișare a configurației grupurilor

Cisco — Compatibilitatea ASA și a componentelor asociate

Cisco — Compatibilitatea FTD și a managerului

Cisco ASA Command Reference — Afișarea informațiilor și fișierelor de crash

Cisco ASA Command Reference — Starea și istoricul failover

Cisco — Planificarea actualizării ASA

Cisco ASA Command Reference — Sesiunile VPN și versiunile software

CISA — Fluxul oficial al catalogului KEV

Limitele evaluării

Nu au fost efectuate scanări, probe de exploatare sau modificări ale echipamentelor beneficiarului. Nu sunt disponibile configurații locale pentru confirmarea activelor afectate. Inventarierea, prioritizarea și matricea de acceptare sunt recomandări ale raportului.

Lipsa unui build dintr-o listă nu demonstrează că este neafectat. Documentația comenzilor se aplică în contextul versiunii și platformei. Nu au fost încărcate documente private ori inventare interne în sursele publice consultate.