CVE-2025-20333, CVE-2025-20362, CVE-2025-20363

Rezumat	Trei vulnerabilităţi critice/înalt-prioritare afectează componente web şi WebVPN ale produselor Cisco (ASA / Secure Firewall FTD / IOS family). Două dintre ele permit execuţie de cod la distanţă (RCE), iar una permite bypass de autorizare (acces neautorizat) la endpoint-uri WebVPN. Exploatare „in-the-wild" a fost confirmată; lanţuri de atac documentate combină bypass pre-auth cu RCE post-auth. Prioritate: critic → aplicaţi patch-urile imediat şi implementaţi măsuri compensatorii dacă patch-ul nu poate fi instalat imediat.
CVE	
CVE-2025-20333- VPN Web Server Remote Code Execution	• Descriere: Vulnerabilitate în VPN Web Server (WebVPN) care poate conduce la execuție de cod la distanță pe dispozitivele afectate când un utilizator malicios exploatează anumite cereri către serviciul WebVPN. Exploatare activă confirmată. • Produse afectate: Cisco Secure Firewall Adaptive Security Appliance (ASA) Software şi Cisco Secure Firewall Threat Defense (FTD) Software (VPN Web Server). • Ramuri / versiuni afectate (sintetizat din source): ✓ ASA: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22. ✓ FTD: 7.0, 7.2, 7.4, 7.6. • Versiuni fixe recomandate: ✓ ASA: 9.16.4.85 · 9.17.1.45 · 9.18.4.47 · 9.19.1.37 · 9.20.3.7 · 9.22.1.3. ✓ FTD: 7.0.8.1 · 7.2.9 · 7.4.2.4 · 7.6.1. • Situație actuală: Confirmată exploatare in-the-wild; atacul necesită cont VPN valid (post-auth). NVD și Cisco mențin evaluarea de RCE pe ASA/FTD. • Lanț tipic: în practică, multe incidente folosesc 20362 (pre-auth bypass) → 20333 (post-auth RCE). (Sinteze Tenable / alți furnizori confirmă inclusiv atribuirea către UAT4356 / Storm-1849). • Condiții de exploatare: ❖ Buffer Overflow prin depășirea limitei de 8192 de octeți pentru câmpul "boundary". ❖ Stack Corruption pentru a controla fluxul de execuție. ❖ Shellcode Execution cu privilegii de root pe dispozitiv.
CVE-2025-20362 — WebVPN access-control bypass (unauthorised access to restricted endpoints)	• Descriere: Vulnerabilitate care permite accesul la endpoint-uri care ar trebui să fie restricționate (bypass de autorizare). Aceasta este adesea folosită ca pas pre-auth/recon înainte de a lansa ulterior RCE (ex.: CVE-20333). Exploatare activă raportată. • Produse afectate: Cisco ASA şi Cisco FTD — componente WebVPN / Web Services. • Ramuri / versiuni afectate: ✓ ASA: 9.16, 9.18, 9.20, 9.22, 9.23. ✓ FTD: 7.0, 7.2, 7.4, 7.6, 7.7. • Versiuni fixe recomandate: ✓ ASA: 9.16.4.85 · 9.18.4.67 · 9.20.4.10 · 9.22.2.14 · 9.23.1.19. ✓ FTD: 7.0.8.1 · 7.2.10.2 · 7.4.2.4 · 7.6.2.1 · 7.7.10.1. • Condiții de exploatare: ❖ Exploatarea se realizează fără autentificare (pre-auth). ❖ Interfața „outside" cu WebVPN activă este suficientă pentru inițierea atacului. ❖ Exploatarea constă în transmiterea unor cereri HTTPS specifice către endpoint-uri WebVPN care nu efectuează verificarea autorizării. ❖ Ocolire mecanisme de autorizare prin manipulare directă a cererilor. ❖ Utilizează cunoștințe despre URI-uri interne ale WebVPN.
CVE-2025-20363 — HTTP Web Services Code Execution	• Descriere: Vulnerabilitate în serviciile web (HTTP/HTTPS) ale unor platforme Cisco (inclusiv IOS/IOS XE/IOS XR şi componente web ale ASA/FTD) care poate permite execuţie de cod la distanţă prin input-uri HTTP nevalidate/încărcare de payload craftat. Documentele vendor menţionează impact atât pe plan de management (HTTP/HTTPS) cât şi pe componente Web Services. • Produse afectate: IOS, IOS XE, IOS XR (module web services); ASA / FTD (componenta web services).

CVE-2025-20333, CVE-2025-20362, CVE-2025-20363

	• Ramuri / versiuni afectate (sintetizat): variază în funcţie de family/version; advisory-urile conţin tabele detaliate pentru fiecare train IOS/ASA/FTD (consultaţi secţiunea „fixed releases" din advisory pentru lista completă).
Impact estimat	• Compromitere completă a dispozitivului (control configurare, trafic, chei, sesiuni). • Lateral movement intern (posibil acces la resurse sensibile), manipulare ACL/NAT, persistence (backdoor). • Operaţiuni critice afectate: conectivitate VPN, acces de management, separarea planurilor de trafic.
Referință	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O https://nvd.nist.gov/vuln/detail/cve-2025-20333 https://nvd.nist.gov/vuln/detail/cve-2025-20362 https://nvd.nist.gov/vuln/detail/CVE-2025-20363