Evaluarea Vulnerabilităților Zero-Day CVE-2025-20333 & CVE-2025-20362 pentru Cisco ASA / FTD

<table>
<tr><td>Rezumat executiv</td><td colspan="3">✓ CVE-2025-20333 (ASA/FTD) – componenta Web/VPN: poate conduce la preluarea completă a dispozitivului când este înlănțuită cu 20362; exploatată ca zero-day.
✓ CVE-2025-20362 (ASA/FTD) – bypass de autorizare către endpoint-uri restricționate; exploatată ca zero-day și folosită adesea ca pas pre-auth pentru 20333.
✓ Activitate atribuită UAT4356 / Storm-1849 (actor cunoscut din campania ArcaneDoor).</td></tr>
<tr><td colspan="4">Versiuni afectate & versiuni fixe</td></tr>
<tr><td>CVE</td><td>Produs</td><td>Ramuri afectate</td><td>Versiuni fixe recomandate</td></tr>
<tr><td>20333</td><td>Cisco ASA</td><td>9.16, 9.17, 9.18, 9.19, 9.20, 9.22</td><td>9.16.4.85 · 9.17.1.45 · 9.18.4.47 · 9.19.1.37 · 9.20.3.7 · 9.22.1.3</td></tr>
<tr><td>20333</td><td>Cisco FTD</td><td>7.0, 7.2, 7.4, 7.6</td><td>7.0.8.1 · 7.2.9 · 7.4.2.4 · 7.6.1</td></tr>
<tr><td>20362</td><td>Cisco ASA</td><td>9.16, 9.18, 9.20, 9.22, 9.23</td><td>9.16.4.85 · 9.18.4.67 · 9.20.4.10 · 9.22.2.14 · 9.23.1.19</td></tr>
<tr><td>20362</td><td>Cisco FTD</td><td>7.0, 7.2, 7.4, 7.6, 7.7</td><td>7.0.8.1 · 7.2.10.2 · 7.4.2.4 · 7.6.2.1 · 7.7.10.1</td></tr>
<tr><td>Exploatare & actor</td><td colspan="3">✓ Exploatare „in the wild” confirmată pentru 20333 și 20362; lanțul (20362 pre-auth → 20333 post-auth) permite compromitere totală.
✓ Atribuire: UAT4356 / Storm-1849, asociat anterior campaniei ArcaneDoor.</td></tr>
<tr><td>IOC</td><td colspan="3">Cisco descrie „Continued Attacks Against Cisco Firewalls”, cu artefacte legate de acces neautorizat la WebVPN și trafic HTTP(S) atipic pe interfața de management/externă. Căutați:
• Jurnale WebVPN cu requests către endpoint-uri neobișnuite sau „restricted URL endpoints” accesate fără autentificare (20362).
• Evenimente crash/restart, core dumps, sau procese nelegitime pornind din contextul web services (20333).
• Autentificări VPN suspecte (imposible travel, IP-uri anonimizate, intervale neobișnuite) urmate de comportament privilegiat.</td></tr>
<tr><td>Detectare & vânătoare de amenințări (ASA/FTD)</td><td colspan="3">✓ Corelați conexiunile către interfața WebVPN (TCP/443) cu URI-uri interne cunoscute ca restricționate; alertați la răspunsuri 200/302 pentru cereri fără sesiune autenticată.
✓ Inspectați syslog/Smart Logging: pattern-uri de input anormal, erori de parsare, excepții în procesele web services după cereri craftate.
✓ Rularea config-audit: verificați expunerea WebVPN pe interfețe neintenționate, management remote permis din segmente publice, și starea patch-urilor.
✓ EDR/NDR: detectați lateral movement dinspre echipament către resurse interne imediat după un access pattern la WebVPN (indicativ de RCE).</td></tr>
<tr><td>Evaluarea riscului (CIA)</td><td colspan="3">✓ Confidențialitate: acces la configurații, credențiale, sesiuni și trafic (post-RCE).
✓ Integritate: injectare de configurări, backdoor firmware, manipularea politicilor ACL/IPS.
✓ Disponibilitate: potențiale crash/restart sau DoS în timpul/după exploatare.
✓ Justificare: natura RCE cu privilegii maxime și bypass de autorizare pe frontiera perimetrală.</td></tr>
<tr><td>Măsuri de remediere</td><td colspan="3">✓ Actualizare software: migrați imediat la versiunile fixe pentru ambele vulnerabilități (și includeți 20363 în fereastra de mentenanță). Planificați rolling upgrades pe clustere HA.
✓ Întărire suprafață WebVPN:
• Expuneți WebVPN numai pe interfețe necesare; separați managementul de data-plane; activați IP allowlist pentru portalul de administrare.
• Dezactivați WebVPN pe interfețe neutilizate; auditați periodic features Web Services.
✓ Autentificare & acces:
• Impuneți MFA pentru toți utilizatorii VPN; revizuiți și curățați conturi inactive.
• Monitorizați anomalii de login (geo-velocity, ASNs suspecte).
✓ Monitorizare & detectare:</td></tr>
</table>

	• Reguli IDS/IPS/WAF pentru pattern-urile de cereri către endpoint-uri restricționate; alertare pe HTTP status anormal (200/302 pe resurse protejate). • Telemetrie consolidată (Syslog, NetFlow) și alerting la reconfigurări neautorizate. ✓ Recuperare & hardening post-incident (dacă IOC-uri sunt prezente): • Factory-reset controlat și reprovisioning din gold image verificată; rotație chei/certificate; reevaluare politicilor ACL/AnyConnect.
Referință	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB?vs_f=Cisco+Security+Advisory%26vs_cat%3DSecurity+Intelligence%26vs_type%3DRSS%26vs_p%3DCisco+Secure+Firewall+Adaptive+Security+Appliance+Software+and+Secure+Firewall+Threat+Defense+Software+VPN+Web+Server+Remote+Code+Execution+Vulnerability%26vs_k%3D1&utm_source=chatgpt.com https://www.tenable.com/blog/cve-2025-20333-cve-2025-20362-faq-cisco-asa-ftd-zero-days-uat4356 https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices?utm_source=chatgpt.com https://www.rapid7.com/blog/post/etr-cve-2025-20333-cve-2025-20362-cve-2025-20363-multiple-critical-vulnerabilities-affecting-cisco-products/?utm_source=chatgpt.com