TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Microsoft termékeket érintő sérülékenységekről

(2025. szeptember 27.)

Tisztelt Ügyfelünk!

A Nemzeti Kiberbiztonsági Intézet riasztást ad ki **a Cisco ASA/FTD tűzfalakat** érintő, több – közülük **kettő aktívan kihasznált** – sérülékenység, valamint a sebezhető eszközök elleni **aktív kibertámadási hullám** kapcsán. A kampány célzottan az ASA/FTD Remote Access VPN/web szolgáltatásait támadja.

Érintett sérülékenységek

- CVE-2025-20333 – ASA/FTD VPN web szerver távoli kódfuttatás (CVSS 9.9), aktívan kihasznált.
- CVE-2025-20362 – ASA/FTD VPN web szerver jogosulatlan hozzáférés (CVSS 6.5), aktívan kihasznált.
- CVE-2025-20363 – ASA/FTD, IOS/IOS XE/IOS XR web szolgáltatások távoli kódfuttatás (CVSS 9.0), nincs információ aktív kihasználásról.

Az eszközök peremvédelmi szerepe miatt a sérülékenységek kihasználása **teljes hálózati kompromittációhoz** vezethet. A támadók képesek lehetnek rosszindulatú komponensek telepítésére és parancsok futtatására az érintett tűzfalakon.

Felhívjuk a figyelmet, hogy kampány során a **támadók ROM manipulációt** is alkalmaznak. Mivel a Secure Boot megléte esetén a Firepower eszközök ezt a technikát észlelik, a **Secure Boot nélküli régebbi ASA 5500-X típusok fokozottan kockázatosak**.

Amennyiben Cisco ASA 5500-X szériájú modellt frissítenek 9.12.4.72, vagy 9.14.4.28 verzióról, kérjük tájékozódjanak az alábbi weboldalon a szükséges információkról az ArcaneDoor kibertámadás detektálási lehetőségei kapcsán:
https://sec.cloudapps.cisco.com/security/center/resources/detection_guide_for_continued_attacks

Amennyiben támadásra utaló jelet tapasztalnak, haladéktalanul vegyék fel a kapcsolatot az NBSZ-NKI CSIRT-el az alábbi elérhetőségen: CSIRT@nki.gov.hu

Érintett rendszerek

Cisco Adaptive Security Appliance (ASA) és Firepower Threat Defense (FTD) szoftvert futtató tűzfalak, különösen ahol engedélyezve van a Remote Access VPN/webes felület.

A Nemzeti Kiberbiztonsági Intézet javasolja ügyfelei számára, hogy **az érintett szoftverek frissítését haladéktalanul hajtsák végre**.

Hivatkozások

- https://cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
- https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_attacks_event_response
- https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks
- https://www.cve.org/CVERecord?id=CVE-2025-20333

TLP:CLEAR
Szabadon terjeszthető!

- https://www.cve.org/CVERecord?id=CVE-2025-20362
- https://www.cve.org/CVERecord?id=CVE-2025-20363
- https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu