TLP:WHITE
Szabadon terjeszthető!

Riasztás
Cisco termékeket érintő sérülékenységekről

(2023. október 24.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki a **Cisco IOS XE** szoftvereket érintő **kritikus, illetve magas kockázati besorolású** sérülékenységek kapcsán, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

A sérülékenységek között **kettő nulladik napi (zero-day)** sebezhetőség található:

- **CVE-2023-20198** Nem megfelelő jogosultságkezelés: A termék nem megfelelően osztja ki, módosítja, követi, vagy ellenőrzi a felhasználói fiókokhoz tartozó jogosultságokat.
- **CVE-2023-20273** A sérülékenység a rendszerhez történő hozzáférés esetén ─ például a korábban publkált CVE-2023-20198 sebezhetőség kihasználásával ─ lehetőséget ad jogosultság-kiterjesztésre, root felhasználói fiók létrehozásával.

Érintett termékek és szerepkörök:

Cisco IOS XE	17.9 17.6 17.3 16.12 (csak a Catalyst 3650 és 3850)

Hibajavítást tartalmazó verziók:

Cisco IOS XE	17.9a 17.6a 17.3a 16.12a

2023.10.24-én csak a 17.9a elérhető, a frissítés állapota a gyártói biztonsági közleményben, itt követhető.

Javaslatok

- **Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.**
- **A gyártói közlemény alapján javasolt a Cisco termékek sebezhetőségeivel összefüggésbe hozható indikátorok alapján kiterjedt vizsgálatot folytatni az esetleges kompromittáltság felderítéséhez.**
- **A támadási felület csökkentése érdekében a http kiszolgáló funkció letiltása az internetkapcsolattal rendelkező rendszereken.**

TLP:WHITE
Szabadon terjeszthető!

Hivatkozások:

- **https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z**
- **https://www.cisa.gov/news-events/alerts/2023/10/23/cisa-updates-guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities**
- **https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2023-20198/**
- **https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2023-20273/**
- **https://nki.gov.hu/it-biztonsag/hirek/figyelem-a-cisco-ujabb-zero-day-serulekenysegre-figyelmeztet/**

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