Upozorňujeme na kritickou zranitelnost CVE-2023-20198 v Cisco IOS XE (CVSS 10.0)

nukib.cz/cs/infoservis/hrozby/2027-upozornujeme-na-kritickou-zranitelnost-cve-2023-20198-v-cisco-ios-xe-cvss-10-0

Národní úřad pro kybernetickou a informační bezpečnost upozorňuje na kritickou zranitelnost CVE-2023-20198, která se týká webového rozhraní operačního systému Cisco IOS XE. Tato zranitelnost umožňuje útočníkovi vytvořit na napadeném zařízení uživatelský účet s úrovní oprávnění "level 15" a tak získat tak kontrolu nad napadenýmdaným zařízením.

Zranitelnost má CVSS Score 10 a je aktivně zneužívána.

Zranitelné systémy:

> Zařízení s operačním systémem CISCO IOS XE, která mají zapnutý modul web UI.

S ohledem na uvedenou zranitelnost doporučujeme postupovat dále uvedeným způsobem.

Mitigace zranitelnosti:

- Vypnout modul web UI.
- V případě, že jej nelze vypnout, omezit jeho dostupnost z internetu i v rámci interní sítě, tj. povolit dostupnost pouze z VLAN určené ke správě těchto zařízení.

Detekce:

Pro ověření, zda je na zařízení modul web UI zapnutý, lze použít příkaz: `show running-config | include ip http server|secure|active`, který blíže popisuje dokumentace ke zranitelnosti od společnosti Cisco. [1]

Daná dokumentace spolu s článkem od Cisco Talos[2] popisuje i indikátory kompromitace, které doporučujeme vyhledat ve zranitelných zařízeních. Ačkoliv jejich výčet není definitivní, mohou pomoci při vyhodnocení závažnosti situace.

Zdroje:

- [1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- [2] https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/