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

portal.neweb.govcert.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-zranitelnost-cve-2023-20198-v-cisco-ios-xe-cvss-10-0

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

Mitigace zranitelnosti

- Vypnout modul web UI.
- Nemít modul web UI dostupný z internetu.
- Omezit jeho dostupnost 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/

Klasifikace

TLP:GREEN

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

18. 10. 2023

Obsah

Reakce

Zatím žádné reakce na článek