Upozornění na zranitelnost CVE-2023-20273 v Cisco IOS XE (CVSS 7.2)

portal.neweb.govcert.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-zranitelnost-cve-2023-20273-v-cisco-ios-xe-cvss-7-2

Národní úřad pro kybernetickou a informační bezpečnost upozorňuje na zranitelnost CVE-2023-20273, která se týká webového rozhraní operačního systému Cisco IOS XE. Tato zranitelnost umožňuje útočníkovi zvýšit oprávnění na úroveň "root". S tímto vysokým oprávněním může nadále instalovat na zařízení vlastní kód.

Zranitelnost má CVSS Score 7.2 a je aktivně zneužívána.

Jedná se o další zranitelnost v tomto systému za uplynulý měsíc. Minulý týden jsme upozornili na kritickou zranitelnost CVE-2023-20198, která umožňuje útočníkům vytvořit na napadeném zařízení účet s oprávněním "level 15" (viz [1]). Po získání prvotního přístupu touto zranitelností, může útočník navázat zneužitím zranitelnosti CVE-2023-20273, čímž si zvýší svá oprávnění.

Mitigace

Dle doporučení společnosti Cisco[2] již byla vydaná verze neobsahující výše zmíněné zranitelnosti:

17.9.4a pro řadu verzí 17.9

Doporučujeme tedy na danou verzi zranitelná zařízení upgradovat a mitigovat možné zneužití v budoucnu omezením přístupu k němu.

Pro ostatní řady verzí není oprava momentálně dostupná. Doporučujeme tedy postupovat v mitigaci a detekci jako v případě zranitelnosti CVE-2023-20198[1].

Zdroje

- [1] https://nukib.cz/cs/infoservis/hrozby/2027-upozornujeme-na-kritickou-zranitelnost-cve-2023-20198-v-cisco-ios-xe-cvss-10-0/
- [2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Klasifikace

TLP:GREEN

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

23. 10. 2023

Obsah

Reakce

Zatím žádné reakce na článek