Kritická zranitelnost Cisco SSM

Upozorňujeme na kritickou zranitelnost s označením CVE-2024-20419 produktu Cisco Smart Software Manager On-Prem (SSM On-Prem) s nejvyšším hodnocením stupně závažnosti (CVSS 10). Tato zranitelnost umožňuje neověřenému vzdálenému útočníkovi měnit hesla všech uživatelů, včetně administrátorských. Je doporučené aktualizovat na novou verzi softwaru, která tuto zranitelnost opravuje. V současné době není známé, že by se tato zranitelnost aktivně využívala. Pro bližší informace o upgradu doporučujeme kontaktovat technickou podporu Cisco TAC.

Zranitelné jsou verze Cisco SSM On-Prem Release 8-202206 a dřívejší, opravené verze 8-202212 a novější. Cisco SSM On-Prem Release verze 9 není zranitelná.

Pokud není možné nyní provést upgrade, je vhodné

1. nastavit síťovou segmentaci k omezení přístupu na SSM On-Prem.
2. Nasadit systém IDS/IPS k monitorování a blokování podezřelých požadavků HTTP zaměřených na změny hesla.
3. Implementovat další mechanismy ověřování, například multifaktor.
4. Pravidelně monitorovat a kontrolovat uživatelské účty, zejména administrátorské, zda nedošlo k jejich neoprávněným změnám.
5. Je-li to možné, dočasně deaktivovat funkci změny hesla, dokud nepřejdete na opravenou verzi produktu, nebo nebude vydaná bezpečnostní záplata.
6. Je vhodné omezit síťový přístup k systému SSM On-Prem pouze na nezbytné a důvěryhodné IP adresy.

Další informace

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy
- https://feedly.com/cve/CVE-2024-20419

Klasifikace

TLP:GREEN

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

18. 07. 2024

Obsah

Reakce

Zatím žádné reakce na článek