Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0315

Kwetsbaarheid verholpen in Cisco Smart Software Manager On-Prem

2024-07-19 Revisie 0

Toegestande verspreiding: TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Cisco heeft een kwetsbaarheid verholpen in Cisco SSM On-Prem (vroeger bekend als Cisco Smart Software Manager Satellite (SSM Satellite).

Interpretaties

De kwetsbaarheid stelt een ongeauthenticeerde kwaadwillende met toegang tot Cisco Smart Software Manager On-Prem in staat om middels het versturen van een HTTP request wachtwoorden te veranderen van gebruikers. Hierbij zou de aanvaller bij succesvol misbruik toegang kunnen krijgen tot de web UI of API met de privileges van desbetreffend gebruiker-account.

Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben.

Oplossingen

Cisco heeft updates beschikbaar gesteld om de kwetsbaarheid te verhelpen. Zie de referenties voor meer informatie.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2024-20419
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy/csaf/cisco-sa-cssm-auth-sLw3uhUy.json
- http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy
- https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html
- https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes
- https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu