



Advisory NCSC-2024-0330

Kwetsbaarheid verholpen in Asterisk

2024-08-12 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.first.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

Er is een kwetsbaarheid verholpen in Asterisk.

Interpretaties

Een kwaadwillende kan de kwetsbaarheid misbruiken om zich verhoogde rechten toe te kennen en willekeurige code uit te voeren met rechten van de applicatie.

Voor succesvol misbruik moet de kwaadwillende over voorafgaande authenticatie beschikken.

De onderzoeker die de kwetsbaarheid heeft ontdekt heeft Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid kan worden aangetoond. De PoC maakt gebruik van een installatie onder controle van de onderzoeker, waardoor omzetten naar exploitcode niet eenvoudig is.

Oplossingen

De ontwikkelaars van Asterisk hebben updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.asterisk.org/downloads/security-advisories/>