Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0386

Kwetsbaarheden verholpen in Zimbra

2024-10-10 Revisie 2

Updates

Revision: 0

Initiele versie

Revision: 1

Dit beveiligingsadvies is naar High/High opgeschaald vanwege een beschikbare exploit en actief misbruik.

Revision: 2

Verwijzing naar NCSC detectie tool voor webshells toegevoegd.

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

Synacor heeft kwetsbaarheden verholpen in Zimbra Collaboration.

Interpretaties

Door middel van het versturen van een speciaal geprepareerde e-mail naar de SMTP server kan direct code executie worden verkregen op de Zimbra server die bijvoorbeeld gebruikt kan worden om een webshell te plaatsen.

Onderzoekers hebben Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-45519 kan worden aangetoond. Er is een exploit beschikbaar en er zijn signalen van actief misbruik.

Oplossingen

UPDATE: Het NCSC heeft op Github een tool beschikbaar gesteld die gebruikt kan worden om een eventuele webshell die middels deze kwetsbaarheid is geplaatst te detecteren.

Synacor heeft updates uitgebracht om de kwetsbaarheden te verhelpen.

Zie bijgevoegde referenties voor meer informatie en de link naar de scantool op Github.

Referenties

- https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
- https://github.com/NCSC-NL/zimbra-webshell-scan