



NCSC-2024-0386

Kwetsbaarheden verholpen in Zimbra

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 10-10-2024

Revisie: 1.0.2

TLP:WHITE

Toegestane verspreiding van 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 van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 2

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

Feiten

Synacor heeft kwetsbaarheden verholpen in Zimbra Collaboration.

Duiding

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>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-38356	
➤ CVE-2024-45194	
➤ CVE-2024-45510	

> CVE-2024-45511	
> CVE-2024-45512	
> CVE-2024-45513	
> CVE-2024-45514	
> CVE-2024-45515	
> CVE-2024-45516	
> CVE-2024-45517	
> CVE-2024-45518	
> CVE-2024-45519	10.0 CRITICAL

CWE's

CWE	Beschrijving
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

synacor
zimbra_collaboration_server
zimbra_collaboration_suite

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.