



NCSC-2024-0438

Kwetsbaarheid verholpen in Microsoft Exchange Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-11-2024

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

Feiten

Microsoft heeft een kwetsbaarheid verholpen in Exchange Server.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop Exchange Server omgaat met P2 FROM headers die niet conform RFC zijn opgebouwd. Een kwaadwillende kan de kwetsbaarheid misbruiken om zich voor te doen als een andere gebruiker en uit naam van het slachtoffer e-mails te versturen.

Hoewel de server zelf weinig risico loopt op misbruik, kan een kwetsbare server misbruikt worden voor phishing-campagnes en andere malafide praktijken.

Aditioneel aan deze update heeft Microsoft ook handelingsperspectieven gepubliceerd om deze kwetsbaarheid, en potentieel misbruik van misvormde P2 FROM headers, tegen te gaan.

Microsoft geeft aan signalen te hebben ontvangen dat informatie over deze kwetsbaarheid wordt gedeeld binnen diverse groepen.

Oplossingen

Microsoft heeft updates beschikbaar gesteld waarmee de beschreven kwetsbaarheden worden verholpen. We raden u aan om deze updates te installeren. Meer informatie over de kwetsbaarheden, de installatie van de updates en eventuele work-arounds vindt u op:

<https://portal.msrc.microsoft.com/en-us/security-guidance>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-49040	

CWE's

CWE	Beschrijving
> CWE-641	Improper Restriction of Names for Files and Other Resources

Getroffen producten

microsoft

exchange_server

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.