Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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.

Additioneel 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