digital trust center.

Ministerie van Economische Zaken

Notificatie kwetsbaarheid in Microsoft Exchange server [DTC]

Geachte heer, mevrouw,

Namens het Digital Trust Center (DTC), onderdeel van het ministerie van Economische Zaken, attenderen wij u op een ernstige cybersecuritydreiging voor uw bedrijf. Dit blijkt uit actuele dreigingsdata waarover we beschikken.

Twijfelt u aan dit bericht? Bezoek onze overheidswebsite en lees hoe u de betrouwbaarheid van het Digital Trust Center als afzender kunt valideren.
https://www.digitaltrustcenter.nl/onderneem-actie
Breng daarnaast uw IT-verantwoordelijke op de hoogte van dit bericht.

Het betreft de volgende cybersecuritydreiging:
Er zijn kwetsbaarheden openbaar gemaakt die het voor een kwaadwillende eventueel mogelijk maken om op Microsoft Exchange Servers willekeurige code uit te voeren[2].

Vanuit betrouwbare bron hebben wij vernomen dat het onderstaand IP-adres(sen) betreft:

{"time.source": "2025-09-23T00:13:37+00:00", "protocol.transport": "", "extra.protocol": "tcp", "source.ip": "127.0.0.1", "source.port": "443", "source.asn": "1136", "source.fqdn": "", "source.reverse_dns": "voorbeeldnotificatiedtc.nl", "extra.version": "15.2.1544.11", "extra.software_version": "", "extra.tag": "cve-2025-53786;exchange", "extra.servername": "EX19"}

Wat kunt u (of uw klant) doen?

• Microsoft heeft updates beschikbaar gesteld [2] om deze kwetsbaarheden te verhelpen. Zorg ervoor dat uw Microsoft Exchange Servers zijn voorzien van de laatste beveiligingsupdates.
• Zorg ervoor dat het betreffende systeem is voorzien van de laatste beveiligingsupdates en Extended Protection is ingeschakeld [3].
Bij exchange versie 2016 en ouder staat extended protection standaard niet ingeschakeld.
• De tag 'eol' staat voor end-of-life. In dat geval is een versie gedetecteerd waar geen beveiligingsupdates meer voor komen. Meer informatie over de risico's van end-of-life software vindt u op [4]
• Verricht technisch onderzoek naar sporen van inbreuk, schade of infectie van andere systemen binnen uw organisatie.
• Controleer uw systemen en verwijder alle verdachte software en bestanden.
• Controleer uw backups op malafide activiteiten en herstel het systeem met een schone backup.
• Onderzoek of kwaadwillenden mogelijk toegang hebben tot meer systemen in uw netwerk.
• Neem contact op met uw IT-dienstverlener als u hierop zelf geen actie kunt ondernemen.
Zie voor meer informatie over hoe deze scan tot stand komt deze pagina van Shadowserver, de bron van de data [5]

Indien u deze notificatie als ISP/dienstverlener krijgt, gaat deze notificatie over een klant van uw bedrijf. Wij vragen u om de klant te informeren die u aan het genoemde IP kunt herleiden.

Wij hopen u hiermee voldoende te hebben geïnformeerd om de dreiging op te lossen. Wanneer u al bekend was met deze dreiging en al actie ondernomen heeft, kunt u deze mail als niet verzonden beschouwen. Mocht u nog vragen hebben over deze notificatie, dan kunt u op deze e-mail reageren.

Tot slot vinden wij het fijn als u wilt laten weten of dit bericht nuttig voor u was. Feedback kunt u bij voorkeur via het feedbackformulier achterlaten wat te vinden is achter onderstaande link [1].

[1] https://www.digitaltrustcenter.nl/feedback-notificatie
[2] https://docs.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates
[3] https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-extended-protection
[4] https://www.digitaltrustcenter.nl/informatie-advies/end-of-life
[5] https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-exchange-server-report

Met vriendelijke groet,
Operator Digital Trust Center (DTC)

.....

algemeen@digitaltrustcenter.nl
www.digitaltrustcenter.nl

+31 70 379 67 00
Postbus 20401 | 2500 EK | Den Haag
Bezuidenhoutseweg 73 | 2594 AC | Den Haag

.....

De privacyverklaring van het Digital Trust Center is te vinden op https://www.digitaltrustcenter.nl/privacy.