Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0289

Kwetsbaarheden verholpen in Microsoft Exchange server

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 28-08-2026
Revisie: 1.0.1

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 1

Voor de kwetsbaarheid met kenmerk CVE-2026-62911 is proof-of-concept-code online verschenen. Deze informatie is aan dit beveiligingsadvies toegevoegd. De aanschaling is bijgesteld van MEDIUM/HIGH naar HIGH/HIGH.

Feiten

Microsoft heeft kwetsbaarheden verholpen in Exchange Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service uit te voeren, zich voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren en/of toegang te krijgen tot gevoelige gegevens.

Update: Voor de kwetsbaarheid met kenmerk CVE-2026-62911 is proof-of-concept-code gepubliceerd. Deze kwetsbaarheid stelt een ongeauthenticeerde kwaadwillende in staat om willekeurige code uit te voeren. Zodoende krijgt de kwaadwillende bijvoorbeeld toegang tot mailboxen van Exchange-gebruikers, en kan de kwetsbaarheid worden misbruikt voor het uitvoeren van verdere aanvallen op het netwerk van het slachtoffer.

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

Houd er rekening mee dat Exchange Server 2016 en 2019 end-of-life zijn en enkel via het ESU-programma nog beveiligingsupdates ontvangen. Het NCSC adviseert met klem om Exchange Servers die geen ESU-ondersteuning ontvangen, alleen vanaf interne netwerken benaderbaar te maken en waar mogelijk uit te faseren.

Referenties

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-62910	7.2 HIGH
CVE-2026-62912	6.5 MEDIUM
CVE-2026-62913	8.8 HIGH
CVE-2026-62914	7.3 HIGH
CVE-2026-62915	6.5 MEDIUM
CVE-2026-65813	6.5 MEDIUM
CVE-2026-62911	8.0 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')
CWE-122	Heap-based Buffer Overflow
CWE-294	Authentication Bypass by Capture-replay
CWE-502	Deserialization of Untrusted Data
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Microsoft
Microsoft Exchange Server 2016 Cumulative Update 23

Microsoft Exchange Server 2019 Cumulative Update 14
Microsoft Exchange Server 2019 Cumulative Update 15
Microsoft Exchange Server Subscription Edition RTM

Disclaimer