Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0252

Kwetsbaarheden verholpen in Microsoft Exchange Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2025

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 kwetsbaarheden verholpen in Microsoft Exchange Server.

Duiding

De kwetsbaarheden in Microsoft Exchange Server zijn het gevolg van onjuiste invoervalidatie en de onjuiste behandeling van speciale elementen, waardoor ongeautoriseerde aanvallers gegevens kunnen manipuleren en communicatie kunnen vervalsen. Dit kan leiden tot ongeautoriseerde toegang, manipulatie van gegevens en blootstelling van gevoelige informatie, wat de integriteit en vertrouwelijkheid van het systeem in gevaar brengt.

```
Microsoft Exchange Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-33051 | 7.50 | Toegang tot gevoelige gegevens      |
| CVE-2025-53786 | 8.00 | Verkrijgen van verhoogde rechten    |
| CVE-2025-25005 | 6.50 | Manipuleren van data      |
| CVE-2025-25006 | 5.30 | Voordoen als andere gebruiker       |
| CVE-2025-25007 | 5.30 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|
```

Oplossingen

Microsoft heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/en-us

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-25005	**6.5 MEDIUM**
CVE-2025-25006	**5.3 MEDIUM**
CVE-2025-25007	**5.3 MEDIUM**

CVE-2025-33051	
CVE-2025-53786	8.0 HIGH

CWE's

CWE	Beschrijving
CWE-167	Improper Handling of Additional Special Element
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-20	Improper Input Validation
CWE-287	Improper Authentication

Getroffen producten

Microsoft
Microsoft Exchange Server Subscription Edition RTM
Microsoft Exchange Server 2019 Cumulative Update 15
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 14

Disclaimer