



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
> <a href="#">CVE-2025-25005</a>	6.5 MEDIUM
> <a href="#">CVE-2025-25006</a>	5.3 MEDIUM
> <a href="#">CVE-2025-25007</a>	5.3 MEDIUM

[> CVE-2025-33051](#)[> CVE-2025-53786](#)**8.0 HIGH**

## CWE's

CWE	Beschrijving
<a href="#">&gt; CVE-167</a>	Improper Handling of Additional Special Element
<a href="#">&gt; CVE-1286</a>	Improper Validation of Syntactic Correctness of Input
<a href="#">&gt; CVE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
<a href="#">&gt; CVE-20</a>	Improper Input Validation
<a href="#">&gt; CVE-287</a>	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

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.