



NCSC-2026-0159

Kwetsbaarheid verholpen in Microsoft Exchange Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-05-2026

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 Microsoft Exchange Server.

Duiding

De kwetsbaarheid betreft een cross-site scripting (XSS) probleem dat ontstaat door onjuiste neutralisatie van invoer tijdens het genereren van webpagina's. Een onbevoegde aanvaller kan hierdoor kwaadaardige scripts injecteren en spoofing-aanvallen uitvoeren over een netwerk. Dit komt doordat gebruikersinvoer onvoldoende wordt gesanitiseerd voordat deze in webpagina's wordt weergegeven. Misbruik van deze kwetsbaarheid kan leiden tot ongeautoriseerde acties binnen de context van de getroffen webapplicatie. De kwetsbaarheid treft specifiek Microsoft Exchange Server omgevingen waar de invoerafhandeling niet adequaat is beveiligd.

Oplossingen

Microsoft heeft, in afwachting van een definitieve oplossing, mitigerende maatregelen geïmplementeerd in de Exchange Emergency Mitigation Service middels een out-of-band update. Deze service is standaard actief. Microsoft adviseert om voor de zekerheid te controleren of deze service daadwerkelijk actief is op de eigen Exchange Server. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-42897	8.1 HIGH

CWE's

CWE	Beschrijving
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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

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.