



NCSC-2026-0349

Kwetsbaarheden verholpen in Microsoft Exchange server

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 08-09-2026

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 9 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.

De ernstigste kwetsbaarheid met kenmerk CVE-2026-69380 heeft een CVSS-score van 9,9 en betreft een autorisatiekwetsbaarheid. Een geauthenticeerde kwaadwillende met beperkte rechten en een toegewezen mailbox kan via het netwerk zijn rechten verhogen en zich voordoen als andere gebruikers. Hierdoor kan de kwaadwillende mailboxen van Exchange-gebruikers overnemen, e-mails lezen en verzenden en bijlagen downloaden.

De kwetsbaarheid met kenmerk CVE-2026-69356 heeft een CVSS-score van 9,3 en betreft een XSS-kwetsbaarheid. Een ongeauthenticeerde kwaadwillende kan een speciaal geprepareerde agenda-uitnodiging versturen. Als een gebruiker de vergaderlink opent, kan de kwaadwillende scripts uitvoeren binnen de Outlook on the Web-sessie en mailboxgegevens inzien of wijzigen.

De kwetsbaarheid met kenmerk CVE-2026-69641 heeft een CVSS-score van 9,1 en betreft een autorisatiekwetsbaarheid. Een geauthenticeerde kwaadwillende met zeer hoge rechten kan via een speciaal geprepareerd verzoek mailboxautorisatiecontroles omzeilen en toegang krijgen tot de mailbox van andere gebruikers. Hierdoor kan de kwaadwillende mailboxen overnemen, e-mails lezen en verzenden en bijlagen downloaden.

Microsoft Exchange Server:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-55007	8,10	Uitvoeren van willekeurige code	
CVE-2026-69355	8,80	Uitvoeren van willekeurige code	
CVE-2026-69356	9,30	Voordoen als andere gebruiker	
CVE-2026-69361	6,50	Voordoen als andere gebruiker	
CVE-2026-69375	6,50	Tampering	
CVE-2026-69378	7,50	Denial-of-Service	
CVE-2026-69380	9,90	Verkrijgen van verhoogde rechten	
CVE-2026-69382	5,90	Toegang tot gevoelige gegevens	
CVE-2026-69641	9,10	Verkrijgen van verhoogde rechten	
-----	-----	-----	

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>

Dreigingsinformatie

Referenties

➤ <https://portal.msrc.microsoft.com/en-us/security-guidance>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-55007	
➤ CVE-2026-69355	
➤ CVE-2026-69356	
➤ CVE-2026-69361	
➤ CVE-2026-69375	
➤ CVE-2026-69378	
➤ CVE-2026-69380	
➤ CVE-2026-69382	
➤ CVE-2026-69641	

CWE's

CWE	Beschrijving
➤ CWE-73	External Control of File Name or Path

➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
➤ CWE-327	Use of a Broken or Risky Cryptographic Algorithm
➤ CWE-415	Double Free
➤ CWE-639	Authorization Bypass Through User-Controlled Key
➤ CWE-674	Uncontrolled Recursion
➤ 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

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.