Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0234

Kwetsbaarheden verholpen in Microsoft Exchange

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-07-2026

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 kwetsbaarheden verholpen in Exchange, zowel Online als on-premise.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen, mogelijk willekeurige code uit te voeren en zo toegang te krijgen tot gevoelige gegevens.

De kwetsbaarheid in Exchange Online is inmiddels door Microsoft centraal verholpen en is opgenomen ter informatie. Hiervoor zijn geen acties benodigd.

De ernstigste kwetsbaarheid in Exchange Server (on-premise) heeft een CVSS van 9.6 toegewezen gekregen en bevindt zich in Outlook Web Access. Deze kwetsbaarheid stelt een kwaadwillende in staat om een Cross-Site-Scripting-aanval (XSS) uit te voeren en zo toegang te krijgen tot de omgeving van het slachtoffer. Er is (nog) geen actief misbruik waargenomen en er is ook geen Proof-of-Concept-code (PoC) bekend, maar Microsoft geeft aan dat zij de kans op misbruik op korte termijn waarschijnlijk achten. Met name OWA-omgevingen die publiek toegankelijk zijn lopen hierdoor verhoogd risico.

```
Microsoft Exchange Online:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-54998 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Microsoft Exchange Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-55005 | 8.80 | Uitvoeren van willekeurige code     |
| CVE-2026-55006 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-55008 | 9.60 | Voordoen als andere gebruiker       |
| CVE-2026-55009 | 7.80 | 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-54998	8.8 HIGH
CVE-2026-55005	8.8 HIGH
CVE-2026-55006	7.8 HIGH
CVE-2026-55008	9.6 CRITICAL
CVE-2026-55009	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-122	Heap-based Buffer Overflow
CWE-502	Deserialization of Untrusted Data
CWE-863	Incorrect Authorization
CWE-1220	Insufficient Granularity of Access Control

Getroffen producten

Microsoft
Microsoft Exchange Online
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