



## Advisory NCSC-2026-0419

PRIORITEIT: NORMAAL

# Kwetsbaarheden verholpen in Microsoft Exchange Server

Publicatiedatum: 13-10-2026

Toegestane verspreiding: TLP:WHITE  
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl).

## Feiten

Microsoft heeft kwetsbaarheden verholpen in Exchange.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen en willekeurige code uit te voeren met rechten van het proces.

Van de kwetsbaarheid met kenmerk CVE-2026-96940 is eerder al een out-of-band update verschenen, maar is ook opgenomen in deze cumulatieve update.

## 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-2026-70279 |            |
| CVE-2026-70571 |            |
| CVE-2026-77910 |            |
| CVE-2026-87692 |            |
| CVE-2026-87695 |            |
| CVE-2026-87696 |            |
| CVE-2026-96940 | 8.8 HIGH   |

## CWE's

| CWE      | Beschrijving                                                                         |
|----------|--------------------------------------------------------------------------------------|
| CWE-79   | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-121  | Stack-based Buffer Overflow                                                          |
| CWE-347  | Improper Verification of Cryptographic Signature                                     |
| CWE-502  | Deserialization of Untrusted Data                                                    |
| CWE-829  | Inclusion of Functionality from Untrusted Control Sphere                             |
| CWE-863  | Incorrect Authorization                                                              |
| CWE-1390 | Weak Authentication                                                                  |

## Getroffen producten

|                                                     |
|-----------------------------------------------------|
| Microsoft                                           |
| Exchange                                            |
| 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 or 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.