Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0425

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft System Center

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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Microsoft heeft kwetsbaarheden verholpen in de Configuration Manager en Defender.

Duiding

Een lokale kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen en mogelijk toegang te krijgen tot gevoelige gegevens.

Microsoft Configuration Manager: |————————|——|————————————————-|

CVE-ID	CVSS	Impact
CVE-2026-88075	8.80	Verkrijgen van verhoogde rechten

————————— ——— ————————————————-

Microsoft Defender for Endpoint: |————————|——|————————————————-|

CVE-ID	CVSS	Impact
CVE-2026-102204	7.80	Verkrijgen van verhoogde rechten

————————— ——— ————————————————-

Microsoft Defender: |————————|——|————————————————-|

CVE-ID	CVSS	Impact
CVE-2026-70264	5.50	Toegang tot gevoelige gegevens

————————— ——— ————————————————-

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-2026-70264	
CVE-2026-88075	
CVE-2026-102204	

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

Microsoft
Microsoft Configuration Manager 2503
Microsoft Configuration Manager 2509
Microsoft Configuration Manager 2603
Microsoft Configuration Manager 2603 on .NET Core 2.1
Microsoft Defender for Endpoint for Linux
Windows Defender

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.