



NCSC-2025-0157

Kwetsbaarheden verholpen in Microsoft Defender

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-05-2025

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 Defender for Endpoint en Defender for Identity.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker en zich verhoogde rechten toe te kennen, waarmee uitvoer van willekeurige code met SYSTEM rechten mogelijk wordt.

Voor succesvol misbruik moet de kwaadwillende lokale toegang tot het kwetsbare systeem hebben, of toegang hebben tot hetzelfde segment in het LAN waar het kwetsbare systeem zich bevindt.

Van de kwetsbaarheid met kenmerk CVE-2025-26685 geeft Microsoft aan informatie te hebben dat deze besproken wordt binnen gesloten fora. Er is (nog) geen publieke Proof-of-Concept vrijgegeven.

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-2025-26684	
> CVE-2025-26685	

CWE's

CWE	Beschrijving
> CWE-73	External Control of File Name or Path
> CWE-287	Improper Authentication

Getroffen producten

Microsoft
Microsoft Defender for Endpoint for Linux
Microsoft Defender for Identity

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.