



# NCSC-2026-0115

## Kwetsbaarheid verholpen in Microsoft Defender

NCSC Advisory

**PRIORITEIT: HOOG**

Gepubliceerd op: 15-04-2026

Revisie: 1.0.1

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

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

## Update Revisie 1

Voor de kwetsbaarheid is een exploit beschikbaar. De inschaling is verhoogd naar High/High

## Feiten

Microsoft heeft een kwetsbaarheid verholpen in System Center.

## Duiding

Een kwaadwillende kan de kwetsbaarheid misbruiken doordat Windows Defender onvoldoende gedetailleerde toegangscontrole toepast, waardoor een geautoriseerde aanvalleur lokaal zijn rechten kan verhogen.

\*\*UPDATE \*\*

Indien Microsoft Defender zichzelf in jouw IT-omgeving automatisch bijwerkt, controleer dan of de desbetreffende beveiligingsupdates zijn geïnstalleerd.

Er is publieke Proof-of-Concept-code (PoC) verschenen die de kwetsbaarheid met kenmerk CVE-2026-33825 aantoont en mogelijk misbruikt. De kans op misbruik neemt hierdoor toe.

## 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
<a href="#">&gt; CVE-2026-33825</a>	7.8 HIGH

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-1220</a>	Insufficient Granularity of Access Control

## Getroffen producten

### **Microsoft**

Microsoft Defender  
Antimalware Platform

## 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.