Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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 aanvaller 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
CVE-2026-33825	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-1220	Insufficient Granularity of Access Control

Getroffen producten

Microsoft
Microsoft Defender Antimalware Platform

Disclaimer