Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0165

Kwetsbaarheid aangetroffen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 20-05-2026

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 maatregelen gepubliceerd voor een kwetsbaarheid in Windows besturingssystemen waarmee lokale kwaadwillenden toegang kunnen krijgen tot data die via BitLocker is versleuteld.

Duiding

De kwetsbaarheid betreft een security feature bypass in Windows, bekend als 'YellowKey'. Er is een proof of concept beschikbaar die aantoont hoe de kwetsbaarheid kan worden misbruikt. De kwetsbaarheid zit niet in de encryptie zelf, maar in de herstelomgeving die BitLocker omringt.

Oplossingen

Microsoft is bezig met het uitbrengen van een security update om de kwetsbaarheid volledig te verhelpen. Tot die tijd zijn er mitigerende maatregelen beschikbaar die als tijdelijke maatregel kunnen worden toegepast. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-45585	**6.8 MEDIUM**

CWE's

CWE	Beschrijving
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

Getroffen producten

Microsoft
Windows 11 Version 24H2
Windows 11 Version 24H2 for x64-based Systems
Windows 11 Version 25H2
Windows 11 Version 25H2 for x64-based Systems
Windows 11 version 26H1
Windows 11 version 26H1 for x64-based Systems
Windows Server 2025
Windows Server 2025 (Server Core installation)

Disclaimer