



NCSC-2026-0141

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-05-2026

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 kwetsbaarheden verholpen in Windows.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Uitvoeren van willekeurige code (root/admin-rechten)
- Uitvoeren van willekeurige code (gebruikersrechten)
- Verkrijgen van verhoogde rechten
- Omzeilen van een beveiligingsmaatregel
- Toegang tot gevoelige gegevens

De ernstigste kwetsbaarheden hebben kenmerken CVE-2026-40402, CVE-2026-41089 en CVE-2026-41096 toegewezen gekregen en bevinden zich respectievelijk in Hyper-V, NETLOGON en de DNS Client. De kwetsbaarheid in Hyper-V stelt een geauthenticeerde kwaadwillende in staat om uit de Guest-VM te breken en toegang te krijgen tot geheugen van de host en mogelijk willekeurige code uit te voeren op de host. De kwetsbaarheden in NETLOGON en de DNS Client stellen een ongeauthenticeerde kwaadwillende op afstand in staat om willekeurige code uit te voeren op het kwetsbare systeem.

Met name Domain Controllers die toegankelijk zijn vanaf externe netwerken lopen een hoog risico voor actief misbruik van de kwetsbaarheid in NETLOGON.

Het verdient altijd aanbeveling om een systeem met de rol van Domain Controller niet publiek toegankelijk te hebben en, indien dit noodzakelijk is, additionele maatregelen te hebben genomen.

Windows Projected File System:

CVE-ID	CVSS	Impact
CVE-2026-34340	7.00	Verkrijgen van verhoogde rechten

Windows Application Identity (AppID) Subsystem:

CVE-ID	CVSS	Impact
CVE-2026-34343	7.80	Verkrijgen van verhoogde rechten

Undisclosed:

CVE-ID	CVSS	Impact
CVE-2026-41095	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop:

CVE-ID	CVSS	Impact
CVE-2026-40398	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows DNS:

CVE-ID	CVSS	Impact
CVE-2026-41096	9.80	Uitvoeren van willekeurige code

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2026-34344	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34345	7.00	Verkrijgen van verhoogde rechten
CVE-2026-35416	7.00	Verkrijgen van verhoogde rechten
CVE-2026-41088	7.80	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2026-33841	7.80	Verkrijgen van verhoogde rechten
CVE-2026-35420	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40369	7.80	Verkrijgen van verhoogde rechten

Windows Secure Boot:

CVE-ID	CVSS	Impact
CVE-2026-41097	6.70	Omzeilen van beveiligingsmaatregel

Windows Native WiFi Miniport Driver:

CVE-ID	CVSS	Impact
CVE-2026-32161	7.50	Uitvoeren van willekeurige code

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact
CVE-2026-40408	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34332	8.00	Uitvoeren van willekeurige code

Telnet Client:

CVE-ID	CVSS	Impact
CVE-2026-35423	5.40	Toegang tot gevoelige gegevens

Windows Print Spooler Components:

CVE-ID	CVSS	Impact
CVE-2026-34342	7.00	Verkrijgen van verhoogde rechten

Windows SMB Client:

CVE-ID	CVSS	Impact
CVE-2026-40410	7.00	Verkrijgen van verhoogde rechten

|-----|-----|-----|

Windows Storage Spaces Controller:

CVE-ID	CVSS	Impact
CVE-2026-35415	7.80	Verkrijgen van verhoogde rechten

Windows Filtering Platform (WFP):

CVE-ID	CVSS	Impact
CVE-2026-32209	4.40	Omzeilen van beveiligingsmaatregel

Windows Volume Manager Extension Driver:

CVE-ID	CVSS	Impact
CVE-2026-40380	6.20	Uitvoeren van willekeurige code

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2026-40377	7.80	Verkrijgen van verhoogde rechten

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2026-33839	7.00	Verkrijgen van verhoogde rechten
CVE-2026-34330	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34331	7.00	Verkrijgen van verhoogde rechten
CVE-2026-34333	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34347	7.00	Verkrijgen van verhoogde rechten
CVE-2026-40403	8.80	Uitvoeren van willekeurige code

Windows Admin Center:

CVE-ID	CVSS	Impact
CVE-2026-35438	8.30	Verkrijgen van verhoogde rechten

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2026-40402	9.30	Verkrijgen van verhoogde rechten

Windows Rich Text Edit Control:

CVE-ID	CVSS	Impact
CVE-2026-32170	6.70	Verkrijgen van verhoogde rechten

Windows Event Logging Service:

CVE-ID	CVSS	Impact
CVE-2026-33834	7.80	Verkrijgen van verhoogde rechten

Windows Internet Key Exchange (IKE) Protocol:

CVE-ID	CVSS	Impact
CVE-2026-35424	7.50	Denial-of-Service

Windows Netlogon:

CVE-ID	CVSS	Impact
CVE-2026-41089	9.80	Uitvoeren van willekeurige code

|-----|-----|-----|

Windows Storport Miniport Driver:

CVE-ID	CVSS	Impact
CVE-2026-34350	6.50	Denial-of-Service

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2026-40407	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40397	7.80	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-35418	7.80	Verkrijgen van verhoogde rechten
CVE-2026-33835	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34337	7.80	Verkrijgen van verhoogde rechten

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2026-33840	7.80	Verkrijgen van verhoogde rechten
CVE-2026-35417	7.80	Verkrijgen van verhoogde rechten

Windows GDI:

CVE-ID	CVSS	Impact
CVE-2026-35421	7.80	Uitvoeren van willekeurige code

Windows Rich Text Edit:

CVE-ID	CVSS	Impact
CVE-2026-21530	6.70	Verkrijgen van verhoogde rechten

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2026-34351	7.80	Verkrijgen van verhoogde rechten
CVE-2026-35422	6.50	Omzeilen van beveiligingsmaatregel
CVE-2026-40399	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40405	7.50	Denial-of-Service
CVE-2026-40406	7.50	Toegang tot gevoelige gegevens
CVE-2026-40414	7.40	Denial-of-Service
CVE-2026-40415	8.10	Uitvoeren van willekeurige code
CVE-2026-33837	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34334	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40401	6.20	Denial-of-Service
CVE-2026-40413	7.40	Denial-of-Service

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2026-34339	5.50	Denial-of-Service

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2026-42825	7.00	Verkrijgen van verhoogde rechten
CVE-2026-34338	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40382	7.80	Verkrijgen van verhoogde rechten

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2026-34329	8.80	Uitvoeren van willekeurige code
CVE-2026-33838	7.80	Verkrijgen van verhoogde rechten

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2026-35419	5.50	Toegang tot gevoelige gegevens
CVE-2026-42896	7.80	Verkrijgen van verhoogde rechten
CVE-2026-34336	7.80	Toegang tot gevoelige gegevens

Windows Link-Layer Discovery Protocol (LLDP):

CVE-ID	CVSS	Impact
CVE-2026-34341	7.00	Verkrijgen van verhoogde rechten

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-2026-34342	7.0 HIGH
> CVE-2026-34343	7.8 HIGH
> CVE-2026-34344	7.8 HIGH

> CVE-2026-34345	7.0 HIGH
> CVE-2026-34347	7.0 HIGH
> CVE-2026-34351	7.8 HIGH
> CVE-2026-35415	7.8 HIGH
> CVE-2026-35416	7.0 HIGH
> CVE-2026-35417	7.8 HIGH
> CVE-2026-35418	7.8 HIGH
> CVE-2026-35421	7.8 HIGH
> CVE-2026-35422	6.5 MEDIUM
> CVE-2026-35423	5.4 MEDIUM
> CVE-2026-35424	7.5 HIGH
> CVE-2026-40377	7.8 HIGH
> CVE-2026-40380	6.2 MEDIUM
> CVE-2026-40399	7.8 HIGH
> CVE-2026-40406	7.5 HIGH
> CVE-2026-40407	7.8 HIGH
> CVE-2026-40408	7.8 HIGH
> CVE-2026-40410	7.0 HIGH
> CVE-2026-40415	8.1 HIGH
> CVE-2026-32161	7.5 HIGH
> CVE-2026-32170	6.7 MEDIUM
> CVE-2026-42825	7.0 HIGH
> CVE-2026-33835	7.8 HIGH

> CVE-2026-33837	7.8 HIGH
> CVE-2026-33838	7.8 HIGH
> CVE-2026-34334	7.8 HIGH
> CVE-2026-34336	7.8 HIGH
> CVE-2026-34337	7.8 HIGH
> CVE-2026-34338	7.8 HIGH
> CVE-2026-34339	5.5 MEDIUM
> CVE-2026-34340	7.0 HIGH
> CVE-2026-34341	7.0 HIGH
> CVE-2026-40382	7.8 HIGH
> CVE-2026-40397	7.8 HIGH
> CVE-2026-32209	4.4 MEDIUM
> CVE-2026-40398	7.8 HIGH
> CVE-2026-40403	8.8 HIGH
> CVE-2026-41097	6.7 MEDIUM
> CVE-2026-40414	7.4 HIGH
> CVE-2026-40401	7.1 HIGH
> CVE-2026-40413	7.4 HIGH
> CVE-2026-35420	7.8 HIGH
> CVE-2026-41089	9.8 CRITICAL
> CVE-2026-41095	7.8 HIGH
> CVE-2026-33841	7.8 HIGH
> CVE-2026-41088	7.8 HIGH

> CVE-2026-40402	9.3 CRITICAL
> CVE-2026-33840	7.8 HIGH
> CVE-2026-34350	6.5 MEDIUM
> CVE-2026-35419	5.5 MEDIUM
> CVE-2026-40405	7.5 HIGH
> CVE-2026-41096	9.8 CRITICAL
> CVE-2026-42896	7.8 HIGH
> CVE-2026-34332	8.0 HIGH
> CVE-2026-40369	7.8 HIGH
> CVE-2026-35438	8.3 HIGH
> CVE-2026-21530	6.7 MEDIUM
> CVE-2026-33834	7.8 HIGH
> CVE-2026-33839	7.0 HIGH
> CVE-2026-34329	8.8 HIGH
> CVE-2026-34330	7.8 HIGH
> CVE-2026-34331	7.0 HIGH
> CVE-2026-34333	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-73	External Control of File Name or Path
> CWE-121	Stack-based Buffer Overflow
> CWE-122	Heap-based Buffer Overflow
> CWE-125	Out-of-bounds Read

➤ CWE-126	Buffer Over-read
➤ CWE-190	Integer Overflow or Wraparound
➤ CWE-191	Integer Underflow (Wrap or Wraparound)
➤ CWE-197	Numeric Truncation Error
➤ CWE-284	Improper Access Control
➤ CWE-288	Authentication Bypass Using an Alternate Path or Channel
➤ CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
➤ CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
➤ CWE-401	Missing Release of Memory after Effective Lifetime
➤ CWE-415	Double Free
➤ CWE-416	Use After Free
➤ CWE-476	NULL Pointer Dereference
➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
➤ CWE-862	Missing Authorization
➤ CWE-1329	Reliance on Component That is Not Updateable

Getroffen producten

Microsoft
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems

Windows 10 Version 1809 for x64-based Systems

Windows 10 Version 21H2 for 32-bit Systems

Windows 10 Version 21H2 for ARM64-based Systems

Windows 10 Version 21H2 for x64-based Systems

Windows 10 Version 22H2 for 32-bit Systems

Windows 10 Version 22H2 for ARM64-based Systems

Windows 10 Version 22H2 for x64-based Systems

Windows 11 Version 23H2 for ARM64-based Systems

Windows 11 Version 23H2 for x64-based Systems

Windows 11 Version 24H2 for ARM64-based Systems

Windows 11 Version 24H2 for x64-based Systems

Windows 11 Version 25H2 for ARM64-based Systems

Windows 11 Version 25H2 for x64-based Systems

Windows 11 Version 26H1 for ARM64-based Systems

Windows 11 Version 26H1 for x64-based Systems

Windows 11 version 26H1 for x64-based Systems

Windows Admin Center
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2022, 23H2 Edition (Server Core installation)
Windows Server 2025
Windows Server 2025 (Server Core installation)

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.