



NCSC-2026-0007

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-01-2026

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)
- Manipulatie van gegevens
- Toegang tot gevoelige gegevens
- Uitvoeren van willekeurige code (gebruikersrechten)
- Uitvoeren van willekeurige code (root/admin)
- Verkrijgen van verhoogde rechten
- Omzeilen van een beveiligingsmaatregel
- Spoofing

Van de kwetsbaarheid met kenmerk CVE-2026-21265 meldt Microsoft informatie te hebben dat deze publiekelijk besproken wordt op fora. Een kwaadwillende kan de kwetsbaarheid misbruiken om Secure Boot te omzeilen. Misbruik is echter niet eenvoudig, vereist voorafgaande verhoogde rechten en een diepgaande kennis van het te compromitteren systeem. Grootschalig misbruik is hiermee zeer onwaarschijnlijk.

Van de kwetsbaarheid met kenmerk CVE-2026-20805 meldt Microsoft dat deze als zeroday-kwetsbaarheid is misbruikt. Misbruik vereist lokale toegang en voorafgaande gebruikersauthenticatie. Verdere informatie is niet bekend gesteld. Grootschalig misbruik is niet waarschijnlijk.

De kwetsbaarheid met kenmerk CVE-2023-31096 is een oudere kwetsbaarheid in Broadcom modem drivers, zoals gebruikt in de (verouderde) Agere modems. Hiervan is al langer Proof-of-Concept-code bekend, maar grootschalig misbruik heeft voor zover bekend nog niet plaatsgevonden. Microsoft heeft in deze update de drivers verwijderd.

Windows Remote Assistance:

----- ----- -----
CVE-ID CVSS Impact
----- ----- -----
CVE-2026-20824 5.50 Omzeilen van beveiligingsmaatregel
----- ----- -----

Capability Access Management Service (camsvc):

----- ----- -----
CVE-ID CVSS Impact

CVE-2026-20815	7.00	Verkrijgen van verhoogde rechten	
CVE-2026-20835	5.50	Toegang tot gevoelige gegevens	
CVE-2026-20851	6.20	Toegang tot gevoelige gegevens	
CVE-2026-20830	7.00	Verkrijgen van verhoogde rechten	
CVE-2026-21221	7.00	Verkrijgen van verhoogde rechten	

Windows Media:

CVE-ID	CVSS	Impact	
CVE-2026-20837	7.80	Uitvoeren van willekeurige code	

Windows Local Session Manager (LSM):

CVE-ID	CVSS	Impact	
CVE-2026-20869	7.00	Verkrijgen van verhoogde rechten	

Windows NDIS:

CVE-ID	CVSS	Impact	
CVE-2026-20936	4.30	Toegang tot gevoelige gegevens	

Windows Management Services:

CVE-ID	CVSS	Impact	
CVE-2026-20858	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20865	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20877	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20918	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20923	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20924	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20861	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20862	5.50	Toegang tot gevoelige gegevens	

CVE-2026-20866	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20867	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20873	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-20874	7.80	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Windows Client-Side Caching (CSC) Service:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20839	5.50	Toegang tot gevoelige gegevens	
-----	-----	-----	

Host Process for Windows Tasks:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20941	7.80	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Graphics Kernel:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20814	7.00	Verkrijgen van verhoogde rechten	
CVE-2026-20836	7.00	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Windows NTLM:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20925	6.50	Voordoen als andere gebruiker	
CVE-2026-20872	6.50	Voordoen als andere gebruiker	
-----	-----	-----	

Windows Ancillary Function Driver for WinSock:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20810	7.80	Verkrijgen van verhoogde rechten	

CVE-2026-20831	7.00	Verkrijgen van verhoogde rechten	
CVE-2026-20860	7.80	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Printer Association Object:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20808	7.00	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Windows Local Security Authority Subsystem Service (LSASS):

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20875	7.50	Denial-of-Service	
CVE-2026-20854	7.50	Uitvoeren van willekeurige code	
-----	-----	-----	

Windows Kernel:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20818	6.20	Toegang tot gevoelige gegevens	
CVE-2026-20838	5.50	Toegang tot gevoelige gegevens	
-----	-----	-----	

Windows Secure Boot:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-21265	6.40	Omzeilen van beveiligingsmaatregel	
-----	-----	-----	

Windows Error Reporting:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20817	7.80	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact
CVE-2026-20859	7.80	Verkrijgen van verhoogde rechten

Windows Remote Procedure Call:

CVE-ID	CVSS	Impact
CVE-2026-20821	6.20	Toegang tot gevoelige gegevens

Dynamic Root of Trust for Measurement (DRTM):

CVE-ID	CVSS	Impact
CVE-2026-20962	4.40	Toegang tot gevoelige gegevens

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2026-20931	8.00	Verkrijgen van verhoogde rechten

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2026-20816	7.80	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2026-20822	7.80	Verkrijgen van verhoogde rechten

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2026-20804	7.70	<Vertaal: Tampering>
CVE-2026-20852	7.70	<Vertaal: Tampering>

Windows WalletService:

CVE-ID	CVSS	Impact
CVE-2026-20853	7.40	Verkrijgen van verhoogde rechten

Desktop Window Manager:

CVE-ID	CVSS	Impact
CVE-2026-20805	5.50	Toegang tot gevoelige gegevens
CVE-2026-20871	7.80	Verkrijgen van verhoogde rechten

Connected Devices Platform Service (Cdpsvc):

CVE-ID	CVSS	Impact
CVE-2026-20864	7.80	Verkrijgen van verhoogde rechten

Windows Internet Connection Sharing (ICS):

CVE-ID	CVSS	Impact
CVE-2026-20828	4.60	Toegang tot gevoelige gegevens

Windows Kerberos:

CVE-ID	CVSS	Impact
--------	------	--------

CVE-2026-20833	5.50	Toegang tot gevoelige gegevens
CVE-2026-20849	7.50	Verkrijgen van verhoogde rechten

Windows Motorola Soft Modem Driver:

CVE-ID	CVSS	Impact
CVE-2024-55414	7.80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2026-20843	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20868	8.80	Uitvoeren van willekeurige code

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2026-20840	7.80	Uitvoeren van willekeurige code
CVE-2026-20922	7.80	Uitvoeren van willekeurige code

Windows DWM:

CVE-ID	CVSS	Impact
CVE-2026-20842	7.00	Verkrijgen van verhoogde rechten

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2026-20825	4.40	Toegang tot gevoelige gegevens

Windows Kernel Memory:

CVE-ID	CVSS	Impact
CVE-2026-20809	7.80	Verkrijgen van verhoogde rechten

Windows Server Update Service:

CVE-ID	CVSS	Impact
CVE-2026-20856	8.10	Uitvoeren van willekeurige code

Windows File Explorer:

CVE-ID	CVSS	Impact
CVE-2026-20823	5.50	Toegang tot gevoelige gegevens
CVE-2026-20932	5.50	Toegang tot gevoelige gegevens
CVE-2026-20937	5.50	Toegang tot gevoelige gegevens
CVE-2026-20939	5.50	Toegang tot gevoelige gegevens

Windows TPM:

CVE-ID	CVSS	Impact
CVE-2026-20829	5.50	Toegang tot gevoelige gegevens

Windows Clipboard Server:

CVE-ID	CVSS	Impact
CVE-2026-20844	7.40	Verkrijgen van verhoogde rechten

Windows Remote Procedure Call Interface Definition Language (IDL):

|--|--|--|

CVE-ID	CVSS	Impact
CVE-2026-20832	7.80	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2026-20820	7.80	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-20857	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20940	7.80	Verkrijgen van verhoogde rechten

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2026-20811	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20920	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20863	7.00	Verkrijgen van verhoogde rechten
CVE-2026-20870	7.80	Verkrijgen van verhoogde rechten

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
CVE-2026-20819	5.50	Toegang tot gevoelige gegevens
CVE-2026-20876	6.70	Verkrijgen van verhoogde rechten
CVE-2026-20938	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20935	6.20	Toegang tot gevoelige gegevens

Agere Windows Modem Driver:

CVE-ID	CVSS	Impact
CVE-2023-31096	7.80	Verkrijgen van verhoogde rechten

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2026-20812	6.50	<Vertaal: Tampering>

Windows HTTP.sys:

CVE-ID	CVSS	Impact
CVE-2026-20929	7.50	Verkrijgen van verhoogde rechten

Windows Deployment Services:

CVE-ID	CVSS	Impact
CVE-2026-0386	7.50	Uitvoeren van willekeurige code

Tablet Windows User Interface (TWINUI) Subsystem:

CVE-ID	CVSS	Impact
CVE-2026-20826	7.80	Verkrijgen van verhoogde rechten
CVE-2026-20827	5.50	Toegang tot gevoelige gegevens

Windows SMB Server:

CVE-ID	CVSS	Impact
CVE-2026-20919	7.50	Verkrijgen van verhoogde rechten
CVE-2026-20921	7.50	Verkrijgen van verhoogde rechten

CVE-2026-20926	7.50	Verkrijgen van verhoogde rechten	
CVE-2026-20927	5.30	Denial-of-Service	
CVE-2026-20934	7.50	Verkrijgen van verhoogde rechten	
CVE-2026-20848	7.50	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Windows Shell:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-20834	4.60	Voordoen als andere gebruiker	
CVE-2026-20847	6.50	Voordoen als andere gebruiker	
-----	-----	-----	

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-2026-20818	6.2 MEDIUM
> CVE-2026-20833	5.5 MEDIUM
> CVE-2026-20920	7.8 HIGH
> CVE-2026-20830	7.0 HIGH
> CVE-2026-20962	4.4 MEDIUM
> CVE-2026-21265	6.4 MEDIUM
> CVE-2026-20804	7.7 HIGH
> CVE-2026-20805	5.5 MEDIUM

> CVE-2026-20808	7.0 HIGH
> CVE-2026-20809	7.8 HIGH
> CVE-2026-20811	7.8 HIGH
> CVE-2026-20812	6.5 MEDIUM
> CVE-2026-20814	7.0 HIGH
> CVE-2026-20815	7.0 HIGH
> CVE-2026-20816	7.8 HIGH
> CVE-2026-20817	7.8 HIGH
> CVE-2026-20819	5.5 MEDIUM
> CVE-2026-20820	7.8 HIGH
> CVE-2026-20821	6.2 MEDIUM
> CVE-2026-20822	7.8 HIGH
> CVE-2026-20823	5.5 MEDIUM
> CVE-2026-20824	5.5 MEDIUM
> CVE-2026-20825	4.4 MEDIUM
> CVE-2026-20826	7.8 HIGH
> CVE-2026-20827	5.5 MEDIUM
> CVE-2026-20828	4.6 MEDIUM
> CVE-2026-20829	5.5 MEDIUM
> CVE-2026-20831	7.8 HIGH
> CVE-2026-20832	7.8 HIGH
> CVE-2026-20834	4.6 MEDIUM
> CVE-2026-20835	5.5 MEDIUM

> CVE-2026-20836	7.0 HIGH
> CVE-2026-20837	7.8 HIGH
> CVE-2026-20838	5.5 MEDIUM
> CVE-2026-20839	5.5 MEDIUM
> CVE-2026-20840	7.8 HIGH
> CVE-2026-20842	7.0 HIGH
> CVE-2026-20844	7.4 HIGH
> CVE-2023-31096	7.8 HIGH
> CVE-2026-20847	6.5 MEDIUM
> CVE-2026-20851	6.2 MEDIUM
> CVE-2026-20852	7.7 HIGH
> CVE-2026-20856	8.1 HIGH
> CVE-2026-20857	7.8 HIGH
> CVE-2026-20858	7.8 HIGH
> CVE-2026-20859	7.8 HIGH
> CVE-2026-20860	7.8 HIGH
> CVE-2026-20864	7.8 HIGH
> CVE-2026-20865	7.8 HIGH
> CVE-2026-20869	7.0 HIGH
> CVE-2026-20875	7.5 HIGH
> CVE-2026-20876	6.7 MEDIUM
> CVE-2026-20877	7.8 HIGH
> CVE-2026-20918	7.8 HIGH

> CVE-2026-20919	7.5 HIGH
> CVE-2026-20921	7.5 HIGH
> CVE-2026-20922	7.8 HIGH
> CVE-2026-20923	7.8 HIGH
> CVE-2026-20924	7.8 HIGH
> CVE-2026-20925	6.5 MEDIUM
> CVE-2026-20926	7.5 HIGH
> CVE-2026-20927	5.3 MEDIUM
> CVE-2026-20932	5.5 MEDIUM
> CVE-2026-20934	7.5 HIGH
> CVE-2026-20938	7.8 HIGH
> CVE-2026-21221	7.0 HIGH
> CVE-2026-20843	7.8 HIGH
> CVE-2026-20848	7.5 HIGH
> CVE-2026-20849	7.5 HIGH
> CVE-2026-20853	7.4 HIGH
> CVE-2026-20854	7.5 HIGH
> CVE-2026-20861	7.8 HIGH
> CVE-2026-20862	5.5 MEDIUM
> CVE-2026-20863	7.0 HIGH
> CVE-2026-20866	7.8 HIGH
> CVE-2026-20867	7.8 HIGH
> CVE-2026-20868	8.8 HIGH

> CVE-2026-20870	7.8 HIGH
> CVE-2026-20871	7.8 HIGH
> CVE-2026-20872	6.5 MEDIUM
> CVE-2026-20873	7.8 HIGH
> CVE-2026-20874	7.8 HIGH
> CVE-2024-55414	9.8 CRITICAL
> CVE-2026-20931	8.0 HIGH
> CVE-2026-20935	6.2 MEDIUM
> CVE-2026-20936	4.3 MEDIUM
> CVE-2026-20937	5.5 MEDIUM
> CVE-2026-20939	5.5 MEDIUM
> CVE-2026-20941	7.8 HIGH
> CVE-2026-20810	7.8 HIGH
> CVE-2026-20940	7.8 HIGH
> CVE-2026-20929	7.5 HIGH
> CVE-2026-0386	7.5 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-36	Absolute Path Traversal
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-73	External Control of File Name or Path

➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-121	Stack-based Buffer Overflow
➤ CWE-122	Heap-based Buffer Overflow
➤ CWE-125	Out-of-bounds Read
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-209	Generation of Error Message Containing Sensitive Information
➤ CWE-266	Incorrect Privilege Assignment
➤ CWE-280	Improper Handling of Insufficient Permissions or Privileges
➤ CWE-284	Improper Access Control
➤ CWE-327	Use of a Broken or Risky Cryptographic Algorithm
➤ CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
➤ CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
➤ CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
➤ CWE-415	Double Free
➤ CWE-416	Use After Free
➤ CWE-476	NULL Pointer Dereference
➤ CWE-532	Insertion of Sensitive Information into Log File
➤ CWE-590	Free of Memory not on the Heap
➤ CWE-693	Protection Mechanism Failure
➤ CWE-807	Reliance on Untrusted Inputs in a Security Decision
➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
➤ CWE-908	Use of Uninitialized Resource
➤ CWE-1329	Reliance on Component That is Not Updateable

Getroffen producten

Microsoft
Windows 10 1607
Windows 10 1809
Windows 10 21h2
Windows 10 22h2
Windows 10 Version 1607
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64- based Systems
Windows 10 Version 1809
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64- based Systems
Windows 10 Version 21H2
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
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 23H2
Windows 11 Version 23H2
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64- based Systems
Windows 11 Version 24H2
Windows 11 Version 24H2 for ARM64-based Systems
Windows 11 Version 24H2 for x64- based Systems
Windows 11 Version 25H2
Windows 11 Version 25H2 for ARM64-based Systems
Windows 11 Version 25H2 for x64- based Systems
Windows 11 version 22H3
Windows Server 2008 R2 Service Pack 1

Windows Server 2008 R2 Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 Service Pack 2
Windows Server 2008 Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
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)
Windows_11_25H2

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.