Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0080

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-03-2026

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)
- Verkrijgen van verhoogde rechten
- Omzeilen van een beveiligingsmaatregel
- Spoofing

```
Windows File Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-24283 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Push Message Routing Service:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-24282 | 5.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Mobile Broadband:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-24288 | 6.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Windows Ancillary Function Driver for WinSock:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

CVE-2026-24293	7.80	Verkrijgen van verhoogde rechten
CVE-2026-25176	7.80	Verkrijgen van verhoogde rechten
CVE-2026-25178	7.00	Verkrijgen van verhoogde rechten
CVE-2026-25179	7.00	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2026-24287	7.80	Verkrijgen van verhoogde rechten
CVE-2026-24289	7.80	Verkrijgen van verhoogde rechten
CVE-2026-26132	7.80	Verkrijgen van verhoogde rechten

Windows Print Spooler Components:

CVE-ID	CVSS	Impact
CVE-2026-23669	8.80	Uitvoeren van willekeurige code

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2026-25167	7.40	Verkrijgen van verhoogde rechten

Windows Resilient File System (ReFS):

CVE-ID	CVSS	Impact
CVE-2026-23673	7.80	Verkrijgen van verhoogde rechten

Windows Telephony Service:

CVE-ID	CVSS	Impact

| CVE-2026-25188 | 8.80 | Verkrijgen van verhoogde rechten |

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2026-23668	7.00	Verkrijgen van verhoogde rechten
CVE-2026-25168	6.20	Denial-of-Service
CVE-2026-25169	6.20	Denial-of-Service
CVE-2026-25180	5.50	Toegang tot gevoelige gegevens

Broadcast DVR:

CVE-ID	CVSS	Impact
CVE-2026-23667	7.00	Verkrijgen van verhoogde rechten

Windows Performance Counters:

CVE-ID	CVSS	Impact
CVE-2026-25165	7.80	Verkrijgen van verhoogde rechten

Windows System Image Manager:

CVE-ID	CVSS	Impact
CVE-2026-25166	7.80	Uitvoeren van willekeurige code

Winlogon:

CVE-ID	CVSS	Impact
CVE-2026-25187	7.80	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2026-24297	6.50	Omzeilen van beveiligingsmaatregel

Windows Authentication Methods:

CVE-ID	CVSS	Impact
CVE-2026-25171	7.00	Verkrijgen van verhoogde rechten

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2026-25175	7.80	Verkrijgen van verhoogde rechten

Windows Universal Disk Format File System Driver (UDFS):

CVE-ID	CVSS	Impact
CVE-2026-23672	7.80	Verkrijgen van verhoogde rechten

Windows Shell Link Processing:

CVE-ID	CVSS	Impact
CVE-2026-25185	5.30	Voordoen als andere gebruiker

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2026-25172	8.80	Uitvoeren van willekeurige code
CVE-2026-25173	8.00	Uitvoeren van willekeurige code

| CVE-2026-26111 | 8.80 | Uitvoeren van willekeurige code |

Windows Bluetooth RFCOM Protocol Driver:

CVE-ID	CVSS	Impact
CVE-2026-23671	7.00	Verkrijgen van verhoogde rechten

Windows Extensible File Allocation:

CVE-ID	CVSS	Impact
CVE-2026-25174	7.80	Verkrijgen van verhoogde rechten

Windows MapUrlToZone:

CVE-ID	CVSS	Impact
CVE-2026-23674	7.50	Omzeilen van beveiligingsmaatregel

Windows Projected File System:

CVE-ID	CVSS	Impact
CVE-2026-24290	7.80	Verkrijgen van verhoogde rechten

Windows Device Association Service:

CVE-ID	CVSS	Impact
CVE-2026-24295	7.00	Verkrijgen van verhoogde rechten
CVE-2026-24296	7.00	Verkrijgen van verhoogde rechten

Connected Devices Platform Service (Cdpsvc):

CVE-ID	CVSS	Impact
CVE-2026-24292	7.80	Verkrijgen van verhoogde rechten

Windows Win32K:

CVE-ID	CVSS	Impact
CVE-2026-24285	7.00	Verkrijgen van verhoogde rechten

Windows App Installer:

CVE-ID	CVSS	Impact
CVE-2026-23656	5.90	Voordoen als andere gebruiker

Windows GDI:

CVE-ID	CVSS	Impact
CVE-2026-25190	7.80	Uitvoeren van willekeurige code

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2026-25170	7.00	Verkrijgen van verhoogde rechten

Windows GDI+:

CVE-ID	CVSS	Impact
CVE-2026-25181	7.50	Toegang tot gevoelige gegevens

Windows Accessibility Infrastructure (ATBroker.exe):

CVE-ID	CVSS	Impact
CVE-2026-24291	7.80	Verkrijgen van verhoogde rechten
CVE-2026-25186	5.50	Toegang tot gevoelige gegevens

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2026-25189	7.80	Verkrijgen van verhoogde rechten

Windows SMB Server:

CVE-ID	CVSS	Impact
CVE-2026-24294	7.80	Verkrijgen van verhoogde rechten
CVE-2026-26128	7.80	Verkrijgen van verhoogde rechten

Active Directory Domain Services:

CVE-ID	CVSS	Impact
CVE-2026-25177	8.80	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-2026-23656	5.9 MEDIUM
CVE-2026-23667	7.0 HIGH
CVE-2026-23668	7.0 HIGH
CVE-2026-23669	8.8 HIGH
CVE-2026-23671	7.0 HIGH
CVE-2026-23672	7.8 HIGH
CVE-2026-23673	7.8 HIGH
CVE-2026-23674	7.5 HIGH
CVE-2026-24282	5.5 MEDIUM
CVE-2026-24283	8.8 HIGH
CVE-2026-24285	7.0 HIGH
CVE-2026-24287	7.8 HIGH
CVE-2026-24288	6.8 MEDIUM
CVE-2026-24289	7.8 HIGH
CVE-2026-24290	7.8 HIGH
CVE-2026-24291	7.8 HIGH
CVE-2026-24292	7.8 HIGH
CVE-2026-24293	7.8 HIGH
CVE-2026-24294	7.8 HIGH
CVE-2026-24295	7.0 HIGH
CVE-2026-24296	7.0 HIGH

CVE-2026-24297	6.5 MEDIUM
CVE-2026-25165	7.8 HIGH
CVE-2026-25166	7.8 HIGH
CVE-2026-25167	7.4 HIGH
CVE-2026-25168	6.2 MEDIUM
CVE-2026-25169	6.2 MEDIUM
CVE-2026-25170	7.0 HIGH
CVE-2026-25171	7.0 HIGH
CVE-2026-25172	8.8 HIGH
CVE-2026-25173	8.0 HIGH
CVE-2026-25174	7.8 HIGH
CVE-2026-25175	7.8 HIGH
CVE-2026-25176	7.8 HIGH
CVE-2026-25177	8.8 HIGH
CVE-2026-25178	7.0 HIGH
CVE-2026-25179	7.0 HIGH
CVE-2026-25180	5.5 MEDIUM
CVE-2026-25181	7.5 HIGH
CVE-2026-25185	5.3 MEDIUM
CVE-2026-25186	5.5 MEDIUM
CVE-2026-25187	7.8 HIGH
CVE-2026-25188	8.8 HIGH
CVE-2026-25189	7.8 HIGH

CVE-2026-25190	7.8 HIGH
CVE-2026-26111	8.8 HIGH
CVE-2026-26128	7.8 HIGH
CVE-2026-26132	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-41	Improper Resolution of Path Equivalence
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-73	External Control of File Name or Path
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-345	Insufficient Verification of Data Authenticity
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-369	Divide By Zero
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-732	Incorrect Permission Assignment for Critical Resource

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 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