Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0213

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-07-2025

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
- Omzeilen van een beveiligingsmaatregel
- Uitvoeren van willekeurige code
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten
- Spoofing

```
Windows Cryptographic Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-48823 | 5.90 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Visual Basic Scripting:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-47159 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Capability Access Management Service (camsvc):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-49690 | 7.40 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Update Service:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

| CVE-2025-48799 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2025-49667	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49733	7.80	Verkrijgen van verhoogde rechten

AMD Store Queue:

CVE-ID	CVSS	Impact
CVE-2025-36350	5.60	Toegang tot gevoelige gegevens

Windows StateRepository API:

CVE-ID	CVSS	Impact
CVE-2025-49723	8.80	Manipulatie van gegevens

Microsoft Windows Search Component:

CVE-ID	CVSS	Impact
CVE-2025-49685	7.00	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2025-49732	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49742	7.80	Uitvoeren van willekeurige code
CVE-2025-49744	7.00	Verkrijgen van verhoogde rechten

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-48002	5.70	Toegang tot gevoelige gegevens
CVE-2025-48822	8.60	Uitvoeren van willekeurige code
CVE-2025-47999	6.80	Denial-of-Service

Microsoft Input Method Editor (IME):

CVE-ID	CVSS	Impact
CVE-2025-47972	8.00	Verkrijgen van verhoogde rechten
CVE-2025-49687	8.80	Verkrijgen van verhoogde rechten
CVE-2025-47991	7.80	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2025-49661	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows QoS scheduler:

CVE-ID	CVSS	Impact
CVE-2025-49730	7.80	Verkrijgen van verhoogde rechten

Windows KDC Proxy Service (KPSSVC):

CVE-ID	CVSS	Impact
CVE-2025-49735	8.10	Uitvoeren van willekeurige code

Windows Print Spooler Components:

CVE-ID	CVSS	Impact
CVE-2025-49722	5.70	Denial-of-Service

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2025-33054	8.10	Voordoen als andere gebruiker
CVE-2025-48817	8.80	Uitvoeren van willekeurige code

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
CVE-2025-48803	6.70	Verkrijgen van verhoogde rechten
CVE-2025-48811	6.70	Verkrijgen van verhoogde rechten

Windows Storage VSP Driver:

CVE-ID	CVSS	Impact
CVE-2025-47982	7.80	Verkrijgen van verhoogde rechten

Windows Cred SSProvider Protocol:

CVE-ID	CVSS	Impact
CVE-2025-47987	7.80	Verkrijgen van verhoogde rechten

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2025-49677	7.00	Verkrijgen van verhoogde rechten

| CVE-2025-49694 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-49693 | 7.80 | Verkrijgen van verhoogde rechten |

AMD L1 Data Queue:

CVE-ID	CVSS	Impact
CVE-2025-36357	5.60	Toegang tot gevoelige gegevens

Windows Connected Devices Platform Service:

CVE-ID	CVSS	Impact
CVE-2025-48000	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49724	8.80	Uitvoeren van willekeurige code

Virtual Hard Disk (VHDX):

CVE-ID	CVSS	Impact
CVE-2025-47971	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49689	7.80	Verkrijgen van verhoogde rechten
CVE-2025-47973	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49683	7.80	Uitvoeren van willekeurige code

Storage Port Driver:

CVE-ID	CVSS	Impact
CVE-2025-49684	5.50	Toegang tot gevoelige gegevens

Windows User-Mode Driver Framework Host:

CVE-ID	CVSS	Impact
CVE-2025-49664	5.50	Toegang tot gevoelige gegevens

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

Windows SmartScreen:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-49740	8.80	Omzeilen van beveiligingsmaatregel

Workspace Broker:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-49665	7.80	Verkrijgen van verhoogde rechten

HID class driver:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-48816	7.80	Verkrijgen van verhoogde rechten

Windows Kerberos:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-47978	6.50	Denial-of-Service

Windows Imaging Component:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-47980	6.20	Toegang tot gevoelige gegevens

Windows TDX.sys:

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

| CVE-2025-49658 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-49659 | 7.80 | Verkrijgen van verhoogde rechten |

Microsoft PC Manager:

CVE-ID	CVSS	Impact
CVE-2025-47993	7.80	Verkrijgen van verhoogde rechten

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-49678	7.00	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-48824	8.80	Uitvoeren van willekeurige code
CVE-2025-49657	8.80	Uitvoeren van willekeurige code
CVE-2025-49670	8.80	Uitvoeren van willekeurige code
CVE-2025-49671	6.50	Toegang tot gevoelige gegevens
CVE-2025-49672	8.80	Uitvoeren van willekeurige code
CVE-2025-49674	8.80	Uitvoeren van willekeurige code
CVE-2025-49676	8.80	Uitvoeren van willekeurige code
CVE-2025-49688	8.80	Uitvoeren van willekeurige code
CVE-2025-49753	8.80	Uitvoeren van willekeurige code
CVE-2025-47998	8.80	Uitvoeren van willekeurige code
CVE-2025-49663	8.80	Uitvoeren van willekeurige code
CVE-2025-49668	8.80	Uitvoeren van willekeurige code
CVE-2025-49669	8.80	Uitvoeren van willekeurige code
CVE-2025-49673	8.80	Uitvoeren van willekeurige code
CVE-2025-49681	6.50	Toegang tot gevoelige gegevens
CVE-2025-49729	8.80	Uitvoeren van willekeurige code

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-26636	5.50	Toegang tot gevoelige gegevens
CVE-2025-48808	5.50	Toegang tot gevoelige gegevens
CVE-2025-48809	5.50	Toegang tot gevoelige gegevens
CVE-2025-49666	7.20	Uitvoeren van willekeurige code

Windows Remote Desktop Licensing Service:

CVE-ID	CVSS	Impact
CVE-2025-48814	7.50	Omzeilen van beveiligingsmaatregel

Windows Fast FAT Driver:

CVE-ID	CVSS	Impact
CVE-2025-49721	7.80	Verkrijgen van verhoogde rechten

Microsoft MPEG-2 Video Extension:

CVE-ID	CVSS	Impact
CVE-2025-48805	7.80	Uitvoeren van willekeurige code
CVE-2025-48806	7.80	Uitvoeren van willekeurige code

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-49727	7.00	Verkrijgen van verhoogde rechten

Universal Print Management Service:

CVE-ID	CVSS	Impact

| CVE-2025-47986 | 8.80 | Verkrijgen van verhoogde rechten |

Windows Media:

CVE-ID	CVSS	Impact
CVE-2025-49691	8.80	Uitvoeren van willekeurige code
CVE-2025-49682	7.30	Verkrijgen van verhoogde rechten

Windows Netlogon:

CVE-ID	CVSS	Impact
CVE-2025-49716	5.90	Denial-of-Service

Windows Event Tracing:

CVE-ID	CVSS	Impact
CVE-2025-47985	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49660	7.80	Verkrijgen van verhoogde rechten

Windows SMB:

CVE-ID	CVSS	Impact
CVE-2025-48802	6.50	Voordoen als andere gebruiker

Windows SPNEGO Extended Negotiation:

CVE-ID	CVSS	Impact
CVE-2025-47981	9.80	Uitvoeren van willekeurige code

Windows Performance Recorder:

CVE-ID	CVSS	Impact
CVE-2025-49680	7.30	Denial-of-Service

Windows Secure Kernel Mode:

CVE-ID	CVSS	Impact
CVE-2025-48810	5.50	Toegang tot gevoelige gegevens

Windows GDI:

CVE-ID	CVSS	Impact
CVE-2025-47984	7.50	Toegang tot gevoelige gegevens

Windows SSDP Service:

CVE-ID	CVSS	Impact
CVE-2025-47976	7.80	Verkrijgen van verhoogde rechten
CVE-2025-47975	7.00	Verkrijgen van verhoogde rechten
CVE-2025-48815	7.80	Verkrijgen van verhoogde rechten

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2025-49686	7.80	Verkrijgen van verhoogde rechten

Kernel Streaming WOW Thunk Service Driver:

CVE-ID	CVSS	Impact

| CVE-2025-49675 | 7.80 | Verkrijgen van verhoogde rechten |

Windows MBT Transport driver:

CVE-ID	CVSS	Impact
CVE-2025-47996	7.80	Verkrijgen van verhoogde rechten

Windows Universal Plug and Play (UPnP) Device Host:

CVE-ID	CVSS	Impact
CVE-2025-48819	7.10	Verkrijgen van verhoogde rechten
CVE-2025-48821	7.10	Verkrijgen van verhoogde rechten

Windows AppX Deployment Service:

CVE-ID	CVSS	Impact
CVE-2025-48820	7.80	Verkrijgen van verhoogde rechten

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2025-48001	6.80	Omzeilen van beveiligingsmaatregel
CVE-2025-48003	6.80	Omzeilen van beveiligingsmaatregel
CVE-2025-48800	6.80	Omzeilen van beveiligingsmaatregel
CVE-2025-48804	6.80	Omzeilen van beveiligingsmaatregel
CVE-2025-48818	6.80	Omzeilen van beveiligingsmaatregel

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2025-49679	7.80	Verkrijgen van verhoogde rechten

```
|----------------|------|-------------------------------------|

Windows Notification:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-49726 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2025-49725 | 7.80 | 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-2025-47998	8.8 HIGH
CVE-2025-48000	7.8 HIGH
CVE-2025-48001	6.8 MEDIUM
CVE-2025-48002	5.7 MEDIUM
CVE-2025-48003	6.8 MEDIUM
CVE-2025-48799	7.8 HIGH
CVE-2025-48800	6.8 MEDIUM
CVE-2025-48803	6.7 MEDIUM
CVE-2025-48804	6.8 MEDIUM
CVE-2025-48805	7.8 HIGH

CVE-2025-48806	7.8 HIGH
CVE-2025-48808	5.5 MEDIUM
CVE-2025-48809	5.5 MEDIUM
CVE-2025-48810	5.5 MEDIUM
CVE-2025-48811	6.7 MEDIUM
CVE-2025-48814	7.5 HIGH
CVE-2025-48815	7.8 HIGH
CVE-2025-48816	7.8 HIGH
CVE-2025-48817	8.8 HIGH
CVE-2025-48818	6.8 MEDIUM
CVE-2025-48819	7.1 HIGH
CVE-2025-48820	7.8 HIGH
CVE-2025-48821	7.1 HIGH
CVE-2025-48822	8.6 HIGH
CVE-2025-48823	5.9 MEDIUM
CVE-2025-49659	7.8 HIGH
CVE-2025-49660	7.8 HIGH
CVE-2025-49663	8.8 HIGH
CVE-2025-49664	5.5 MEDIUM
CVE-2025-49665	7.8 HIGH
CVE-2025-49666	7.2 HIGH
CVE-2025-49667	7.8 HIGH
CVE-2025-49668	8.8 HIGH

CVE-2025-49669	8.8 HIGH
CVE-2025-49673	8.8 HIGH
CVE-2025-49675	7.8 HIGH
CVE-2025-49678	7.0 HIGH
CVE-2025-49679	7.8 HIGH
CVE-2025-49680	7.3 HIGH
CVE-2025-49681	6.5 MEDIUM
CVE-2025-49682	7.3 HIGH
CVE-2025-49683	7.8 HIGH
CVE-2025-49684	5.5 MEDIUM
CVE-2025-49693	7.8 HIGH
CVE-2025-49722	5.7 MEDIUM
CVE-2025-49724	8.8 HIGH
CVE-2025-49725	7.8 HIGH
CVE-2025-49727	7.0 HIGH
CVE-2025-49729	8.8 HIGH
CVE-2025-49730	7.8 HIGH
CVE-2025-49732	7.8 HIGH
CVE-2025-49733	7.8 HIGH
CVE-2025-47999	6.8 MEDIUM
CVE-2025-49740	8.8 HIGH
CVE-2025-49742	7.8 HIGH
CVE-2025-49744	7.0 HIGH

CVE-2025-49677	7.0 HIGH
CVE-2025-48802	6.5 MEDIUM
CVE-2025-49685	7.0 HIGH
CVE-2025-49716	5.9 MEDIUM
CVE-2025-26636	5.5 MEDIUM
CVE-2025-33054	8.1 HIGH
CVE-2025-47159	7.8 HIGH
CVE-2025-47971	7.8 HIGH
CVE-2025-47972	8.0 HIGH
CVE-2025-47976	7.8 HIGH
CVE-2025-47984	7.5 HIGH
CVE-2025-47985	7.8 HIGH
CVE-2025-47986	8.8 HIGH
CVE-2025-47987	7.8 HIGH
CVE-2025-48824	8.8 HIGH
CVE-2025-49657	8.8 HIGH
CVE-2025-49658	5.5 MEDIUM
CVE-2025-49661	7.8 HIGH
CVE-2025-49670	8.8 HIGH
CVE-2025-49671	6.5 MEDIUM
CVE-2025-49672	8.8 HIGH
CVE-2025-49674	8.8 HIGH
CVE-2025-49676	8.8 HIGH

CVE-2025-49686	7.8 HIGH
CVE-2025-49687	8.8 HIGH
CVE-2025-49688	8.8 HIGH
CVE-2025-49689	7.8 HIGH
CVE-2025-49690	7.4 HIGH
CVE-2025-49691	8.8 HIGH
CVE-2025-49694	7.8 HIGH
CVE-2025-47991	7.8 HIGH
CVE-2025-47993	7.8 HIGH
CVE-2025-36357	
CVE-2025-36350	
CVE-2025-49721	7.8 HIGH
CVE-2025-49723	8.8 HIGH
CVE-2025-49726	7.8 HIGH
CVE-2025-49735	8.1 HIGH
CVE-2025-49753	8.8 HIGH
CVE-2025-47973	7.8 HIGH
CVE-2025-47975	7.0 HIGH
CVE-2025-47978	6.5 MEDIUM
CVE-2025-47980	6.2 MEDIUM
CVE-2025-47981	9.8 CRITICAL
CVE-2025-47982	7.8 HIGH
CVE-2025-47996	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-353	Missing Support for Integrity Check
CWE-1037	Processor Optimization Removal or Modification of Security-critical Code
CWE-197	Numeric Truncation Error
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-820	Missing Synchronization
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-357	Insufficient UI Warning of Dangerous Operations
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-23	Relative Path Traversal
CWE-190	Integer Overflow or Wraparound
CWE-693	Protection Mechanism Failure
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-284	Improper Access Control
CWE-416	Use After Free

CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-400	Uncontrolled Resource Consumption
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow

Getroffen producten

Microsoft
Remote Desktop client for Windows Desktop
Windows 10 Version 1507
Windows 10 Version 1607
Windows 10 Version 1809
Windows 10 Version 21H2
Windows 10 Version 22H2
Windows 11 Version 23H2
Windows 11 Version 24H2
Windows 11 version 22H2
Windows 11 version 22H3
Windows App Client for Windows Desktop

Windows Server 2008 Service Pack 2
Windows Server 2008 R2 Service Pack 1
Windows Server 2008 R2 Service Pack 1 (Server Core installation)
Windows Server 2008 Service Pack 2
Windows Server 2008 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, 23H2 Edition (Server Core installation)
Windows Server 2025

Windows Server 2025 (Server Core installation)

Disclaimer