Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0078

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-03-2025

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)
- Omzeilen van beveiligingsmaatregel
- Uitvoer van willekeurige code (root/adminrechten)
- Uitvoer van willekeurige code (Gebruikersrechten)
- Verkrijgen van verhoogde rechten
- Toegang tot gevoelige gegevens
- Voordoen als andere gebruiker

Van de kwetsbaarheden met kenmerk CVE-2025-24983, CVE-2025-24984, CVE-2025-24985, CVE-2025-24991, CVE-2025-24993 en CVE-2025-26633 geeft Microsoft aan informatie te hebben dat deze eerder actief zijn misbruikt als Zeroday. Er is geen publieke Proof-of-Concept (PoC) of exploitcode bekend. De kwetsbaarheden zijn uitsluitend lokaal te misbruiken. Grootschalig actief misbruik wordt hierdoor niet waarschijnlijk geacht.

```
Windows Kernel-Mode Drivers:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-24066 | 8.40 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Remote Desktop Client:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-26645 | 8.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Kernel Streaming WOW Thunk Service Driver:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-24995 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows USB Video Driver:

CVE-ID	CVSS	Impact
CVE-2025-24987	6.60	Verkrijgen van verhoogde rechten
CVE-2025-24988	6.60	Verkrijgen van verhoogde rechten
CVE-2025-24055	4.30	Toegang tot gevoelige gegevens

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-24051	8.80	Uitvoeren van willekeurige code

Role: DNS Server:

CVE-ID	CVSS	Impact
CVE-2025-24064	8.10	Uitvoeren van willekeurige code

Microsoft Management Console:

CVE-ID	CVSS	Impact
CVE-2025-26633	7.00	Omzeilen van beveiligingsmaatregel

Windows exFAT File System:

CVE-ID	CVSS	Impact
CVE-2025-21180	7.80	Uitvoeren van willekeurige code

Windows Cross Device Service:

CVE-ID	CVSS	Impact

CVE-2025-24076	7.30	Verkrijgen van verhoogde rechten
CVE-2025-24994	7.30	Verkrijgen van verhoogde rechten

Windows Fast FAT Driver:

CVE-ID	CVSS	Impact
CVE-2025-24985	7.80	Uitvoeren van willekeurige code

Microsoft Windows:

CVE-ID	CVSS	Impact
CVE-2024-9157	onb.	Verkrijgen van verhoogde rechten
CVE-2025-25008	7.10	Verkrijgen van verhoogde rechten

Windows Mark of the Web (MOTW):

CVE-ID	CVSS	Impact
CVE-2025-24061	7.80	Omzeilen van beveiligingsmaatregel

Windows Win32 Kernel Subsystem:

CVE-ID	CVSS	Impact
CVE-2025-24044	7.80	Verkrijgen van verhoogde rechten
CVE-2025-24983	7.00	Verkrijgen van verhoogde rechten

Windows Kernel Memory:

CVE-ID	CVSS	Impact
CVE-2025-24997	4.40	Denial-of-Service

Microsoft Local Security Authority Server (lsasrv):

CVE-ID	CVSS	Impact
CVE-2025-24072	7.80	Verkrijgen van verhoogde rechten

Microsoft Streaming Service:

CVE-ID	CVSS	Impact
CVE-2025-24046	7.80	Verkrijgen van verhoogde rechten
CVE-2025-24067	7.80	Verkrijgen van verhoogde rechten

Windows Telephony Server:

CVE-ID	CVSS	Impact
CVE-2025-24056	8.80	Uitvoeren van willekeurige code

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2025-24996	6.50	Voordoen als andere gebruiker
CVE-2025-24054	6.50	Voordoen als andere gebruiker

Windows MapUrlToZone:

CVE-ID	CVSS	Impact
CVE-2025-21247	4.30	Omzeilen van beveiligingsmaatregel

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact

| CVE-2025-24059 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-24048	7.80	Verkrijgen van verhoogde rechten
CVE-2025-24050	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop Services:

CVE-ID	CVSS	Impact
CVE-2025-24035	8.10	Uitvoeren van willekeurige code
CVE-2025-24045	8.10	Uitvoeren van willekeurige code

Windows Subsystem for Linux:

CVE-ID	CVSS	Impact
CVE-2025-24084	8.40	Uitvoeren van willekeurige code

Windows File Explorer:

CVE-ID	CVSS	Impact
CVE-2025-24071	7.50	Voordoen als andere gebruiker

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-24984	4.60	Toegang tot gevoelige gegevens
CVE-2025-24991	5.50	Toegang tot gevoelige gegevens
CVE-2025-24992	5.50	Toegang tot gevoelige gegevens

```
| CVE-2025-24993 | 7.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

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-2025-24035	
CVE-2024-9157	7.8 HIGH
CVE-2025-24044	7.8 HIGH
CVE-2025-24987	
CVE-2025-24988	
CVE-2025-21180	
CVE-2025-24995	
CVE-2025-24996	
CVE-2025-21247	
CVE-2025-24046	
CVE-2025-24051	
CVE-2025-24054	
CVE-2025-24055	
CVE-2025-24056	8.8 HIGH

CVE-2025-24059	7.8 HIGH
CVE-2025-24061	
CVE-2025-24066	
CVE-2025-24067	
CVE-2025-24071	
CVE-2025-24072	7.8 HIGH
CVE-2025-24984	
CVE-2025-24985	
CVE-2025-24991	
CVE-2025-24992	
CVE-2025-24993	
CVE-2025-26633	
CVE-2025-26645	
CVE-2025-24048	
CVE-2025-24050	7.8 HIGH
CVE-2025-25008	
CVE-2025-24045	
CVE-2025-24064	
CVE-2025-24997	
CVE-2025-24084	8.4 HIGH
CVE-2025-24076	
CVE-2025-24994	
CVE-2025-24983	

CWE's

CWE	Beschrijving
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-707	Improper Neutralization
CWE-41	Improper Resolution of Path Equivalence
CWE-23	Relative Path Traversal
CWE-190	Integer Overflow or Wraparound
CWE-693	Protection Mechanism Failure
CWE-532	Insertion of Sensitive Information into Log File
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-73	External Control of File Name or Path
CWE-681	Incorrect Conversion between Numeric Types

Getroffen producten

Microsoft
Remote Desktop client for Windows Desktop

Windows
Windows 10 1507
Windows 10 1607
Windows 10 1809
Windows 10 21h2
Windows 10 22h2
Windows 11 22H2
Windows 11 23H2
Windows 11 Version 24H2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server 2022
Windows Server 2025
Windows Server 23H2
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 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 (Server Core installation)
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016 (Server Core installation)

Windows Server 2019 (Server Core installation)
Windows Server 2022, 23H2 Edition (Server Core installation)
Windows Server 2025 (Server Core installation)

Disclaimer