Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0277

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2025

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 een beveiligingsmaatregel
- Uitvoer van willekeurige code (root/adminrechten)
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten

Van de kwetsbaarheid met kenmerk CVE-2025-55234 geeft Microsoft aan dat details publiek bekend zijn. Er is (nog) geen Proof-of-Concept-code (PoC) of exploit beschikbaar. De kwetsbaarheid bevindt zich in SMB en stelt een ongeauthenticeerde kwaadwillende in staat om zich de rechten van het slachtoffer toe te eigenen. Hiervoor moet de kwaadwillende het slachtoffer misleiden om acties uit te voeren, zoals het volgen van een link of openen van een bestand.

```
Capability Access Management Service (camsvc):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-54108 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows BitLocker:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-54911 | 7.30 | Verkrijgen van verhoogde rechten    |
| CVE-2025-54912 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Management Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
```

| CVE-2025-54103 | 7.40 | Verkrijgen van verhoogde rechten |

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-54919	7.50	Uitvoeren van willekeurige code
CVE-2025-55228	7.80	Uitvoeren van willekeurige code
CVE-2025-55224	7.80	Uitvoeren van willekeurige code

Graphics Kernel:

CVE-ID	CVSS	Impact
CVE-2025-55223	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55226	6.70	Uitvoeren van willekeurige code
CVE-2025-55236	7.30	Uitvoeren van willekeurige code

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2025-54918	8.80	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2025-54099	7.00	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-54110	8.80	Verkrijgen van verhoogde rechten
CVE-2025-53803	5.50	Toegang tot gevoelige gegevens

CVE-2025-53804	5.50	Toegang tot gevoelige gegevens

Windows Bluetooth Service:

CVE-ID	CVSS	Impact
CVE-2025-53802	7.00	Verkrijgen van verhoogde rechten

Windows DWM:

CVE-ID	CVSS	Impact
CVE-2025-53801	7.80	Verkrijgen van verhoogde rechten

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2025-54105	7.00	Verkrijgen van verhoogde rechten

Windows Connected Devices Platform Service:

CVE-ID	CVSS	Impact
CVE-2025-54102	7.80	Verkrijgen van verhoogde rechten
CVE-2025-54114	7.00	Denial-of-Service

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2025-53800	7.80	Verkrijgen van verhoogde rechten
CVE-2025-53807	7.00	Verkrijgen van verhoogde rechten

Windows MultiPoint Services:

CVE-ID	CVSS	Impact
CVE-2025-54116	7.30	Verkrijgen van verhoogde rechten

Windows UI XAML Maps MapControlSettings:

CVE-ID	CVSS	Impact
CVE-2025-54913	7.80	Verkrijgen van verhoogde rechten

Windows Defender Firewall Service:

CVE-ID	CVSS	Impact
CVE-2025-53808	6.70	Verkrijgen van verhoogde rechten
CVE-2025-53810	6.70	Verkrijgen van verhoogde rechten
CVE-2025-54094	6.70	Verkrijgen van verhoogde rechten
CVE-2025-54104	6.70	Verkrijgen van verhoogde rechten
CVE-2025-54109	6.70	Verkrijgen van verhoogde rechten
CVE-2025-54915	6.70	Verkrijgen van verhoogde rechten

Windows Imaging Component:

CVE-ID	CVSS	Impact
CVE-2025-53799	5.50	Toegang tot gevoelige gegevens

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-53797	6.50	Toegang tot gevoelige gegevens
CVE-2025-53798	6.50	Toegang tot gevoelige gegevens
CVE-2025-54095	6.50	Toegang tot gevoelige gegevens
CVE-2025-54096	6.50	Toegang tot gevoelige gegevens
CVE-2025-54097	6.50	Toegang tot gevoelige gegevens

CVE-2025-54106	8.80	Uitvoeren van willekeurige code
CVE-2025-55225	6.50	Toegang tot gevoelige gegevens
CVE-2025-53796	6.50	Toegang tot gevoelige gegevens
CVE-2025-53806	6.50	Toegang tot gevoelige gegevens
CVE-2025-54113	7.50	Uitvoeren van willekeurige code

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-54916	7.80	Uitvoeren van willekeurige code

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-54091	7.80	Verkrijgen van verhoogde rechten
CVE-2025-54092	7.80	Verkrijgen van verhoogde rechten
CVE-2025-54098	7.80	Verkrijgen van verhoogde rechten
CVE-2025-54115	7.00	Verkrijgen van verhoogde rechten

Windows PowerShell:

CVE-ID	CVSS	Impact
CVE-2025-49734	7.00	Verkrijgen van verhoogde rechten

Microsoft Virtual Hard Drive:

CVE-ID	CVSS	Impact
CVE-2025-54112	7.00	Verkrijgen van verhoogde rechten

Windows MapUrlToZone:

| CVE-ID | CVSS | Impact |

| CVE-2025-54107 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-54917 | 4.30 | Omzeilen van beveiligingsmaatregel |

Windows SMB:

CVE-ID	CVSS	Impact
CVE-2025-55234	8.80	Verkrijgen van verhoogde rechten

Windows SPNEGO Extended Negotiation:

CVE-ID	CVSS	Impact
CVE-2025-54895	7.80	Verkrijgen van verhoogde rechten

Windows Internet Information Services:

CVE-ID	CVSS	Impact
CVE-2025-53805	7.50	Denial-of-Service

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2025-54093	7.00	Verkrijgen van verhoogde rechten

Windows Local Security Authority Subsystem Service (LSASS):

CVE-ID	CVSS	Impact
CVE-2025-54894	7.80	Verkrijgen van verhoogde rechten
CVE-2025-53809	6.50	Denial-of-Service

```
Windows SMBv3 Client:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-54101 | 4.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Windows UI XAML Phone DatePickerFlyout:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-54111 | 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-2025-49734	7.0 HIGH
CVE-2025-54099	7.0 HIGH
CVE-2025-54101	4.8 MEDIUM
CVE-2025-54102	7.8 HIGH
CVE-2025-54110	8.8 HIGH
CVE-2025-54111	7.8 HIGH
CVE-2025-54894	7.8 HIGH
CVE-2025-54895	7.8 HIGH

CVE-2025-54913	7.8 HIGH
CVE-2025-54916	7.8 HIGH
CVE-2025-54918	8.8 HIGH
CVE-2025-54919	7.5 HIGH
CVE-2025-55223	7.0 HIGH
CVE-2025-55226	
CVE-2025-55236	
CVE-2025-53799	5.5 MEDIUM
CVE-2025-53800	7.8 HIGH
CVE-2025-53801	7.8 HIGH
CVE-2025-53803	5.5 MEDIUM
CVE-2025-53804	5.5 MEDIUM
CVE-2025-53807	7.0 HIGH
CVE-2025-53808	6.7 MEDIUM
CVE-2025-53810	6.7 MEDIUM
CVE-2025-54093	7.0 HIGH
CVE-2025-54094	6.7 MEDIUM
CVE-2025-54104	6.7 MEDIUM
CVE-2025-54107	4.3 MEDIUM
CVE-2025-54109	6.7 MEDIUM
CVE-2025-54112	7.0 HIGH
CVE-2025-54116	7.3 HIGH
CVE-2025-54911	7.3 HIGH

CVE-2025-54912	7.8 HIGH
CVE-2025-54915	6.7 MEDIUM
CVE-2025-54917	4.3 MEDIUM
CVE-2025-55234	
CVE-2025-54091	7.8 HIGH
CVE-2025-54092	7.8 HIGH
CVE-2025-54098	7.8 HIGH
CVE-2025-54115	7.0 HIGH
CVE-2025-55224	7.8 HIGH
CVE-2025-53797	6.5 MEDIUM
CVE-2025-53798	6.5 MEDIUM
CVE-2025-54095	6.5 MEDIUM
CVE-2025-54096	6.5 MEDIUM
CVE-2025-54097	6.5 MEDIUM
CVE-2025-54106	8.8 HIGH
CVE-2025-55225	6.5 MEDIUM
CVE-2025-53796	6.5 MEDIUM
CVE-2025-53806	6.5 MEDIUM
CVE-2025-54113	8.8 HIGH
CVE-2025-55228	
CVE-2025-53802	7.0 HIGH
CVE-2025-53805	7.5 HIGH
CVE-2025-54114	7.0 HIGH

CVE-2025-54103	7.4 HIGH
CVE-2025-53809	6.5 MEDIUM
CVE-2025-54105	7.0 HIGH
CVE-2025-54108	7.0 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-41	Improper Resolution of Path Equivalence
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-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-416	Use After Free
CWE-693	Protection Mechanism Failure
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-908	Use of Uninitialized Resource

CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-1419	Incorrect Initialization of Resource

Getroffen producten

Microsoft
Windows 10
Windows 10 1607
Windows 10 1809
Windows 10 21h2
Windows 10 22h2
Windows 10 Version 1507
Windows 10 Version 1607
Windows 10 Version 1809
Windows 10 Version 21H2
Windows 10 Version 22H2
Windows 11 22H2
Windows 11 23H2
Windows 11 Version 23H2

Windows 11 Version 24H2
Windows 11 version 22H2
Windows 11 version 22H3
Windows Server 2008
Windows Server 2008 Service Pack 2
Windows Server 2008 R2
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