Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0358

Kwetsbaartheden verholpen in Microsoft Windows

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

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
- Uitvoeren van willekeurige code (root/adminrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten

De ernstigste kwetsbaarheid heeft kenmerk CVE-2025-60724 toegewezen gekregen en bevindt zich in de GDI+ Graphics Component. Deze kwetsbaarheid stelt een kwaadwillende in staat om willekeurige code uit te voeren op het kwetsbare systeem. Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bestand te downloaden en te openen. In beperkte omstandigheden is het voor een kwaadwillende ook mogelijk om de kwetsbaarheid te misbruiken op bijvoorbeeld een publiek toegankelijke webservice, door het uploaden van een malfide bestand. Hiervoor is verder geen gebruikerinteractie benodigd.

```
Windows DirectX:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-59506 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2025-60716 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2025-60723 | 6.30 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows Administrator Protection:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-60718 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2025-60721 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Customer Experience Improvement Program (CEIP):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
```

| CVE-2025-59512 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Bluetooth RFCOM Protocol Driver:

CVE-ID	CVSS	Impact
CVE-2025-59513	5.50	Toegang tot gevoelige gegevens

Windows License Manager:

CVE-ID	CVSS	Impact
CVE-2025-62208	5.50	Toegang tot gevoelige gegevens
CVE-2025-62209	5.50	Toegang tot gevoelige gegevens

Windows Remote Desktop:

CVE-ID	CVSS	Impact
CVE-2025-60703	7.80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-59510	5.50	Denial-of-Service
CVE-2025-62452	8.00	Uitvoeren van willekeurige code
CVE-2025-60713	7.80	Verkrijgen van verhoogde rechten
CVE-2025-60715	8.00	Uitvoeren van willekeurige code

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-60706	5.50	Toegang tot gevoelige gegevens

Windows Speech:

CVE-ID	CVSS	Impact
CVE-2025-59507	7.00	Verkrijgen van verhoogde rechten
CVE-2025-59508	7.00	Verkrijgen van verhoogde rechten
CVE-2025-59509	5.50	Toegang tot gevoelige gegevens

Multimedia Class Scheduler Service (MMCSS):

CVE-ID	CVSS	Impact
CVE-2025-60707	7.80	Verkrijgen van verhoogde rechten

Windows Smart Card:

CVE-ID	CVSS	Impact
CVE-2025-59505	7.80	Verkrijgen van verhoogde rechten

Windows TDX.sys:

CVE-ID	CVSS	Impact
CVE-2025-60720	7.80	Verkrijgen van verhoogde rechten

Windows OLE:

CVE-ID	CVSS	Impact
CVE-2025-60714	7.80	Uitvoeren van willekeurige code

Windows Kernel:

CVE-ID	CVSS	Impact

| CVE-2025-62215 | 7.00 | Verkrijgen van verhoogde rechten |

Windows WLAN Service:

CVE-ID	CVSS	Impact
CVE-2025-59511	7.80	Verkrijgen van verhoogde rechten

Microsoft Streaming Service:

CVE-ID	CVSS	Impact
CVE-2025-59514	7.80	Verkrijgen van verhoogde rechten

Host Process for Windows Tasks:

CVE-ID	CVSS	Impact
CVE-2025-60710	7.80	Verkrijgen van verhoogde rechten

Windows Client-Side Caching (CSC) Service:

CVE-ID	CVSS	Impact
CVE-2025-60705	7.80	Verkrijgen van verhoogde rechten

Windows Broadcast DVR User Service:

CVE-ID	CVSS	Impact
CVE-2025-59515	7.00	Verkrijgen van verhoogde rechten
CVE-2025-60717	7.00	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2025-60719	7.00	Verkrijgen van verhoogde rechten
CVE-2025-62217	7.00	Verkrijgen van verhoogde rechten
CVE-2025-62213	7.00	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2025-60709	7.80	Verkrijgen van verhoogde rechten

Microsoft Wireless Provisioning System:

CVE-ID	CVSS	Impact
CVE-2025-62218	7.00	Verkrijgen van verhoogde rechten
CVE-2025-62219	7.00	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2025-60724	9.80	Uitvoeren van willekeurige code

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2025-60704	7.50	Verkrijgen van verhoogde rechten

Storvsp.sys Driver:

CVE-ID	CVSS	Impact

```
| CVE-2025-60708 | 6.50 | Denial-of-Service                  |
|----------------|------|------------------------------------|
```

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-2025-59505	7.8 HIGH
CVE-2025-59506	7.0 HIGH
CVE-2025-59507	7.0 HIGH
CVE-2025-59508	7.0 HIGH
CVE-2025-59509	5.5 MEDIUM
CVE-2025-59510	5.5 MEDIUM
CVE-2025-59511	7.8 HIGH
CVE-2025-59512	7.8 HIGH
CVE-2025-59513	5.5 MEDIUM
CVE-2025-60703	7.8 HIGH
CVE-2025-60704	7.5 HIGH
CVE-2025-60705	7.8 HIGH
CVE-2025-60707	7.8 HIGH
CVE-2025-60709	7.8 HIGH

CVE-2025-60719	7.0 HIGH
CVE-2025-62217	7.0 HIGH
CVE-2025-62218	7.0 HIGH
CVE-2025-62219	7.0 HIGH
CVE-2025-59514	7.8 HIGH
CVE-2025-59515	7.0 HIGH
CVE-2025-60713	7.8 HIGH
CVE-2025-60714	7.8 HIGH
CVE-2025-60715	8.0 HIGH
CVE-2025-60716	7.0 HIGH
CVE-2025-60717	7.0 HIGH
CVE-2025-60720	7.8 HIGH
CVE-2025-60723	6.3 MEDIUM
CVE-2025-60724	9.8 CRITICAL
CVE-2025-62208	5.5 MEDIUM
CVE-2025-62209	5.5 MEDIUM
CVE-2025-62215	7.0 HIGH
CVE-2025-62213	7.0 HIGH
CVE-2025-60706	5.5 MEDIUM
CVE-2025-60708	6.5 MEDIUM
CVE-2025-62452	8.0 HIGH
CVE-2025-60710	7.8 HIGH
CVE-2025-60718	7.8 HIGH

CVE-2025-60721	7.8 HIGH

CWE's

CWE	Beschrijving
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-126	Buffer Over-read
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-269	Improper Privilege Management
CWE-270	Privilege Context Switching Error
CWE-284	Improper Access Control
CWE-325	Missing Cryptographic Step
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-415	Double Free
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-532	Insertion of Sensitive Information into Log File
CWE-822	Untrusted Pointer Dereference

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 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 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 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 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)

Disclaimer