Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0112

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-04-2025

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 kwetsbaarheid met kenmerk CVE-2025-29824 geeft Microsoft aan dat deze eerder actief is misbruikt als zero-day. Er is geen publieke Proof-of-Concept (PoC) of exploitcode bekend. Een kwaadwillende die met succes deze kwetsbaarheid misbruikt, zou SYSTEM-rechten kunnen verkrijgen.

```
Windows Subsystem for Linux:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-26675 | 7,80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows upnphost.dll:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-26665 | 7,00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Mark of the Web (MOTW):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-27472 | 5,40 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|
```

Windows Remote Desktop Services:

CVE-ID	CVSS	Impact
CVE-2025-26671	8,10	Uitvoeren van willekeurige code

Windows Update Stack:

CVE-ID	CVSS	Impact
CVE-2025-21204	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27475	7,00	Verkrijgen van verhoogde rechten

Windows Mobile Broadband:

CVE-ID	CVSS	Impact
CVE-2025-29811	7,80	Verkrijgen van verhoogde rechten

Windows Standards-Based Storage Management Service:

CVE-ID	CVSS	Impact
CVE-2025-27470	7,50	Denial-of-Service
CVE-2025-27486	7,50	Denial-of-Service
CVE-2025-26652	7,50	Denial-of-Service
CVE-2025-26680	7,50	Denial-of-Service
CVE-2025-27485	7,50	Denial-of-Service
CVE-2025-21174	7,50	Denial-of-Service

Windows Digital Media:

CVE-ID	CVSS	Impact
CVE-2025-26640	7,00	Verkrijgen van verhoogde rechten
CVE-2025-27467	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27476	7,80	Verkrijgen van verhoogde rechten

| CVE-2025-27730 | 7,80 | Verkrijgen van verhoogde rechten |

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-26648	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27739	7,80	Verkrijgen van verhoogde rechten

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2025-27487	8,00	Uitvoeren van willekeurige code

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
CVE-2025-27735	6,00	Omzeilen van beveiligingsmaatregel

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact
CVE-2025-27728	7,80	Verkrijgen van verhoogde rechten

Windows Resilient File System (ReFS):

CVE-ID	CVSS	Impact
CVE-2025-27738	6,50	Toegang tot gevoelige gegevens

Windows Active Directory Certificate Services:

CVE-ID	CVSS	Impact
CVE-2025-27740	8,80	Verkrijgen van verhoogde rechten

Windows Power Dependency Coordinator:

CVE-ID	CVSS	Impact
CVE-2025-27736	5,50	Toegang tot gevoelige gegevens

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2025-27727	7,80	Verkrijgen van verhoogde rechten

Windows Bluetooth Service:

CVE-ID	CVSS	Impact
CVE-2025-27490	7,80	Verkrijgen van verhoogde rechten

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2025-26635	6,50	Omzeilen van beveiligingsmaatregel
CVE-2025-26644	6,20	Voordoen als andere gebruiker

Windows Local Security Authority (LSA):

CVE-ID	CVSS	Impact
CVE-2025-21191	7,00	Verkrijgen van verhoogde rechten
CVE-2025-27478	7,00	Verkrijgen van verhoogde rechten

RPC Endpoint Mapper Service:

CVE-ID	CVSS	Impact
CVE-2025-26679	7,80	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2025-29809	7,10	Omzeilen van beveiligingsmaatregel
CVE-2025-26647	8,10	Voordoen als andere gebruiker
CVE-2025-27479	7,50	Denial-of-Service

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2025-26641	7,50	Denial-of-Service
CVE-2025-29808	5,50	Toegang tot gevoelige gegevens

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-27483	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27742	5,50	Toegang tot gevoelige gegevens
CVE-2025-21197	6,50	Toegang tot gevoelige gegevens
CVE-2025-27733	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27741	7,80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-26667	6,50	Toegang tot gevoelige gegevens

CVE-2025-26672	6,50	Toegang tot gevoelige gegevens
CVE-2025-26676	6,50	Toegang tot gevoelige gegevens
CVE-2025-27474	6,50	Toegang tot gevoelige gegevens
CVE-2025-21203	6,50	Toegang tot gevoelige gegevens
CVE-2025-26664	6,50	Toegang tot gevoelige gegevens
CVE-2025-26668	7,50	Uitvoeren van willekeurige code
CVE-2025-26669	8,80	Toegang tot gevoelige gegevens

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-27491	7,10	Uitvoeren van willekeurige code

Microsoft Streaming Service:

CVE-ID	CVSS	Impact
CVE-2025-27471	5,90	Denial-of-Service

Windows Kernel Memory:

CVE-ID	CVSS	Impact
CVE-2025-29812	7,80	Verkrijgen van verhoogde rechten

Microsoft Virtual Hard Drive:

CVE-ID	CVSS	Impact
CVE-2025-26688	7,80	Verkrijgen van verhoogde rechten

Windows Security Zone Mapping:

CVE-ID	CVSS	Impact

| CVE-2025-27737 | 8,60 | Omzeilen van beveiligingsmaatregel |

OpenSSH for Windows:

CVE-ID	CVSS	Impact
CVE-2025-27731	7,80	Verkrijgen van verhoogde rechten

Windows Secure Channel:

CVE-ID	CVSS	Impact
CVE-2025-27492	7,00	Verkrijgen van verhoogde rechten
CVE-2025-26649	7,00	Verkrijgen van verhoogde rechten

Remote Desktop Gateway Service:

CVE-ID	CVSS	Impact
CVE-2025-27480	8,10	Uitvoeren van willekeurige code
CVE-2025-27482	8,10	Uitvoeren van willekeurige code

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-26681	6,70	Verkrijgen van verhoogde rechten
CVE-2025-26687	7,50	Verkrijgen van verhoogde rechten
CVE-2025-27732	7,00	Verkrijgen van verhoogde rechten

Windows Media:

CVE-ID	CVSS	Impact
CVE-2025-26666	7,80	Uitvoeren van willekeurige code
CVE-2025-26674	7,80	Uitvoeren van willekeurige code

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

Windows Common Log File System Driver:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-29824	7,80	Verkrijgen van verhoogde rechten

Windows HTTP.sys:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-27473	7,50	Denial-of-Service

Windows Local Session Manager (LSM):

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-26651	6,50	Denial-of-Service

Windows USB Print Driver:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-26639	7,80	Verkrijgen van verhoogde rechten

Windows TCP/IP:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-26686	7,50	Uitvoeren van willekeurige code

Windows LDAP - Lightweight Directory Access Protocol:

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

CVE-2025-26670	8,10	Uitvoeren van willekeurige code
CVE-2025-27469	7,50	Denial-of-Service
CVE-2025-26663	8,10	Uitvoeren van willekeurige code
CVE-2025-26673	7,50	Denial-of-Service

Windows Universal Plug and Play (UPnP) Device Host:

CVE-ID	CVSS	Impact
CVE-2025-27484	7,50	Verkrijgen van verhoogde rechten

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2025-21205	8,80	Uitvoeren van willekeurige code
CVE-2025-21221	8,80	Uitvoeren van willekeurige code
CVE-2025-21222	8,80	Uitvoeren van willekeurige code
CVE-2025-27477	8,80	Uitvoeren van willekeurige code
CVE-2025-27481	8,80	Uitvoeren van willekeurige code

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2025-24073	7,80	Verkrijgen van verhoogde rechten
CVE-2025-24062	7,80	Verkrijgen van verhoogde rechten
CVE-2025-24058	7,80	Verkrijgen van verhoogde rechten
CVE-2025-24074	7,80	Verkrijgen van verhoogde rechten
CVE-2025-24060	7,80	Verkrijgen van verhoogde rechten

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2025-26637	6,80	Omzeilen van beveiligingsmaatregel, Verkrijgen van verhoogde rechten

Windows Defender Application Control (WDAC):

CVE-ID	CVSS	Impact
CVE-2025-26678	8,40	Omzeilen van beveiligingsmaatregel

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2025-27729	7,80	Uitvoeren van willekeurige code

Active Directory Domain Services:

CVE-ID	CVSS	Impact
CVE-2025-29810	7,50	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

Dreigingsinformatie

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-21174	7.5 HIGH
CVE-2025-21191	7.0 HIGH

CVE-2025-21197	6.5 MEDIUM
CVE-2025-21203	6.5 MEDIUM
CVE-2025-21204	7.8 HIGH
CVE-2025-21205	8.8 HIGH
CVE-2025-21221	8.8 HIGH
CVE-2025-21222	8.8 HIGH
CVE-2025-24058	7.8 HIGH
CVE-2025-24060	7.8 HIGH
CVE-2025-24062	7.8 HIGH
CVE-2025-24073	7.8 HIGH
CVE-2025-24074	7.8 HIGH
CVE-2025-26635	6.5 MEDIUM
CVE-2025-26637	6.8 MEDIUM
CVE-2025-26639	7.8 HIGH
CVE-2025-26640	7.0 HIGH
CVE-2025-26641	7.5 HIGH
CVE-2025-26644	5.1 MEDIUM
CVE-2025-26647	8.1 HIGH
CVE-2025-26648	7.8 HIGH
CVE-2025-26649	7.0 HIGH
CVE-2025-26651	6.5 MEDIUM
CVE-2025-26652	7.5 HIGH
CVE-2025-26663	8.1 HIGH

CVE-2025-26664	6.5 MEDIUM
CVE-2025-26665	7.0 HIGH
CVE-2025-26666	7.8 HIGH
CVE-2025-26667	6.5 MEDIUM
CVE-2025-26668	7.5 HIGH
CVE-2025-26669	8.8 HIGH
CVE-2025-26670	8.1 HIGH
CVE-2025-26671	8.1 HIGH
CVE-2025-26672	6.5 MEDIUM
CVE-2025-26673	7.5 HIGH
CVE-2025-26674	7.8 HIGH
CVE-2025-26675	7.8 HIGH
CVE-2025-26676	6.5 MEDIUM
CVE-2025-26678	8.4 HIGH
CVE-2025-26679	7.8 HIGH
CVE-2025-26680	7.5 HIGH
CVE-2025-26681	6.7 MEDIUM
CVE-2025-26686	7.5 HIGH
CVE-2025-26687	7.5 HIGH
CVE-2025-26688	7.8 HIGH
CVE-2025-27467	7.8 HIGH
CVE-2025-27469	7.5 HIGH
CVE-2025-27470	7.5 HIGH

CVE-2025-27471	5.9 MEDIUM
CVE-2025-27472	5.4 MEDIUM
CVE-2025-27473	7.5 HIGH
CVE-2025-27474	6.5 MEDIUM
CVE-2025-27475	7.0 HIGH
CVE-2025-27476	7.8 HIGH
CVE-2025-27477	8.8 HIGH
CVE-2025-27478	7.0 HIGH
CVE-2025-27479	7.5 HIGH
CVE-2025-27480	8.1 HIGH
CVE-2025-27481	8.8 HIGH
CVE-2025-27482	8.1 HIGH
CVE-2025-27483	7.8 HIGH
CVE-2025-27484	7.5 HIGH
CVE-2025-27485	7.5 HIGH
CVE-2025-27486	7.5 HIGH
CVE-2025-27487	8.0 HIGH
CVE-2025-27490	7.8 HIGH
CVE-2025-27491	7.1 HIGH
CVE-2025-27492	7.0 HIGH
CVE-2025-27727	7.8 HIGH
CVE-2025-27728	7.8 HIGH
CVE-2025-27729	7.8 HIGH

CVE-2025-27730	7.8 HIGH
CVE-2025-27731	7.8 HIGH
CVE-2025-27732	7.0 HIGH
CVE-2025-27733	7.8 HIGH
CVE-2025-27735	6.0 MEDIUM
CVE-2025-27736	5.5 MEDIUM
CVE-2025-27737	8.6 HIGH
CVE-2025-27738	6.5 MEDIUM
CVE-2025-27739	7.8 HIGH
CVE-2025-27740	8.8 HIGH
CVE-2025-27741	7.8 HIGH
CVE-2025-27742	5.5 MEDIUM
CVE-2025-29808	5.5 MEDIUM
CVE-2025-29809	7.1 HIGH
CVE-2025-29810	7.5 HIGH
CVE-2025-29811	7.8 HIGH
CVE-2025-29812	7.8 HIGH
CVE-2025-29824	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation

CWE-749	Exposed Dangerous Method or Function
CWE-1390	Weak Authentication
CWE-1039	Inadequate Detection or Handling of Adversarial Input Perturbations in Automated Recognition Mechanism
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-922	Insecure Storage of Sensitive Information
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-410	Insufficient Resource Pool
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-908	Use of Uninitialized Resource
CWE-345	Insufficient Verification of Data Authenticity
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-284	Improper Access Control
CWE-416	Use After Free
CWE-400	Uncontrolled Resource Consumption
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-20	Improper Input Validation

Getroffen producten

Microsoft
Microsoft Office for Android
Microsoft Office for Universal
Remote Desktop client for Windows Desktop
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 App Client for Windows Desktop
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)
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)

Disclaimer