Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0053

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-02-2026

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

```
Desktop Window Manager:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-21519 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Mailslot File System:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-21253 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows LDAP - Lightweight Directory Access Protocol:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-21243 | 7.50 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows Kernel:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

|----------------|------|-------------------------------------|
CVE-2026-21245	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21239	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21231	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21222	5.50	Toegang tot gevoelige gegevens

Windows Remote Desktop:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-21533	7.80	Verkrijgen van verhoogde rechten

Windows Remote Access Connection Manager:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-21525	6.20	Denial-of-Service

Windows Shell:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-21510	8.80	Omzeilen van beveiligingsmaatregel

Role: Windows Hyper-V:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-21248	7.30	Uitvoeren van willekeurige code
CVE-2026-21247	7.30	Uitvoeren van willekeurige code
CVE-2026-21255	8.80	Omzeilen van beveiligingsmaatregel
CVE-2026-21244	7.30	Uitvoeren van willekeurige code

Windows Win32K - GRFX:

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

| CVE-2023-2804 | 6.50 | Uitvoeren van willekeurige code |

Windows Cluster Client Failover:

CVE-ID	CVSS	Impact
CVE-2026-21251	7.80	Verkrijgen van verhoogde rechten

Windows HTTP.sys:

CVE-ID	CVSS	Impact
CVE-2026-21250	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21240	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21232	7.80	Verkrijgen van verhoogde rechten

Windows Connected Devices Platform Service:

CVE-ID	CVSS	Impact
CVE-2026-21234	7.00	Verkrijgen van verhoogde rechten

Windows GDI+:

CVE-ID	CVSS	Impact
CVE-2026-20846	7.50	Denial-of-Service

Windows App for Mac:

CVE-ID	CVSS	Impact
CVE-2026-21517	7.00	Verkrijgen van verhoogde rechten

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2026-21249	3.30	Voordoen als andere gebruiker

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2026-21236	7.80	Verkrijgen van verhoogde rechten
CVE-2026-21241	7.00	Verkrijgen van verhoogde rechten
CVE-2026-21238	7.80	Verkrijgen van verhoogde rechten

Internet Explorer:

CVE-ID	CVSS	Impact
CVE-2026-21513	8.80	Omzeilen van beveiligingsmaatregel

Windows Storage:

CVE-ID	CVSS	Impact
CVE-2026-21508	7.00	Verkrijgen van verhoogde rechten

Windows Subsystem for Linux:

CVE-ID	CVSS	Impact
CVE-2026-21242	7.00	Verkrijgen van verhoogde rechten
CVE-2026-21237	7.00	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact

```
|----------------|------|-------------------------------------|
| CVE-2026-21246 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-21235 | 7.30 | 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-2026-21519	7.8 HIGH
CVE-2026-21246	7.8 HIGH
CVE-2026-21235	7.3 HIGH
CVE-2026-21234	7.0 HIGH
CVE-2026-21236	7.8 HIGH
CVE-2026-21533	7.8 HIGH
CVE-2026-21513	8.8 HIGH
CVE-2026-21510	8.8 HIGH
CVE-2026-21525	6.2 MEDIUM
CVE-2026-21508	7.0 HIGH
CVE-2026-21253	7.0 HIGH
CVE-2026-21249	3.3 LOW
CVE-2026-21240	7.8 HIGH

CVE-2026-21239	7.8 HIGH
CVE-2026-21238	7.8 HIGH
CVE-2026-21231	7.8 HIGH
CVE-2026-21222	5.5 MEDIUM
CVE-2026-20846	7.5 HIGH
CVE-2026-21248	7.3 HIGH
CVE-2026-21247	7.3 HIGH
CVE-2026-21255	8.8 HIGH
CVE-2026-21244	7.3 HIGH
CVE-2026-21251	7.8 HIGH
CVE-2026-21243	7.5 HIGH
CVE-2026-21242	7.0 HIGH
CVE-2026-21241	7.0 HIGH
CVE-2026-21237	7.0 HIGH
CVE-2026-21250	7.8 HIGH
CVE-2026-21245	7.8 HIGH
CVE-2026-21232	7.8 HIGH
CVE-2023-2804	6.5 MEDIUM
CVE-2026-21517	7.0 HIGH
CVE-2026-20841	8.8 HIGH

CWE's

CWE	Beschrijving

CWE-20	Improper Input Validation
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-73	External Control of File Name or Path
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-269	Improper Privilege Management
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-426	Untrusted Search Path
CWE-476	NULL Pointer Dereference
CWE-532	Insertion of Sensitive Information into Log File
CWE-693	Protection Mechanism Failure
CWE-787	Out-of-bounds Write
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')

Getroffen producten

Microsoft
Windows 10 1607

Windows 10 1809
Windows 10 21h2
Windows 10 22h2
Windows 10 Version 1607
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64- based Systems
Windows 10 Version 1809
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64- based Systems
Windows 10 Version 21H2
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
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 11 23H2
Windows 11 Version 23H2
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows 11 Version 24H2
Windows 11 Version 24H2 for ARM64-based Systems
Windows 11 Version 24H2 for x64-based Systems
Windows 11 Version 25H2
Windows 11 Version 25H2 for ARM64-based Systems
Windows 11 Version 25H2 for x64-based Systems
Windows 11 Version 26H1
Windows 11 Version 26H1 for ARM64-based Systems
Windows 11 version 22H3
Windows 11 version 26H1
Windows 11 version 26H1 for x64-based Systems

Windows App for Mac
Windows Notepad
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