Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0119

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-04-2026

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

```
Function Discovery Service (fdwsd.dll):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-32087 | 7,00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-32093 | 7,00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-32086 | 7,00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-32150 | 7,00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Applocker Filter Driver (applockerfltr.sys):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-25184 | 7,00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Kernel:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-26179 | 7,80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-26180 | 7,80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-32195 | 7,00 | Verkrijgen van verhoogde rechten    |
```

CVE-2026-32215	5,50	Toegang tot gevoelige gegevens
CVE-2026-32217	5,50	Toegang tot gevoelige gegevens
CVE-2026-32218	5,50	Toegang tot gevoelige gegevens
CVE-2026-26163	7,80	Verkrijgen van verhoogde rechten

Windows Remote Procedure Call:

CVE-ID	CVSS	Impact
CVE-2026-32085	5,50	Toegang tot gevoelige gegevens

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2026-32070	7,00	Verkrijgen van verhoogde rechten

Microsoft Management Console:

CVE-ID	CVSS	Impact
CVE-2026-27914	7,80	Verkrijgen van verhoogde rechten

Windows Push Notification Core:

CVE-ID	CVSS	Impact
CVE-2026-26167	8,80	Verkrijgen van verhoogde rechten
CVE-2026-32158	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32159	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32160	7,80	Verkrijgen van verhoogde rechten
CVE-2026-26172	7,80	Verkrijgen van verhoogde rechten

Windows Installer:

| CVE-ID | CVSS | Impact |

| CVE-2026-27910 | 7,80 | Verkrijgen van verhoogde rechten |

Windows File Explorer:

CVE-ID	CVSS	Impact
CVE-2026-32081	5,50	Toegang tot gevoelige gegevens
CVE-2026-32079	5,50	Toegang tot gevoelige gegevens
CVE-2026-32084	5,50	Toegang tot gevoelige gegevens

Windows Boot Manager:

CVE-ID	CVSS	Impact
CVE-2026-26175	4,60	Omzeilen van beveiligingsmaatregel

Windows Boot Loader:

CVE-ID	CVSS	Impact
CVE-2026-0390	6,70	Omzeilen van beveiligingsmaatregel

Windows User Interface Core:

CVE-ID	CVSS	Impact
CVE-2026-32165	7,80	Verkrijgen van verhoogde rechten
CVE-2026-27911	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32163	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32164	7,80	Verkrijgen van verhoogde rechten

Microsoft Windows Speech:

CVE-ID	CVSS	Impact

| CVE-2026-32153 | 7,80 | Verkrijgen van verhoogde rechten |

Windows USB Print Driver:

CVE-ID	CVSS	Impact
CVE-2026-32223	6,80	Verkrijgen van verhoogde rechten

Windows COM:

CVE-ID	CVSS	Impact
CVE-2026-20806	5,50	Toegang tot gevoelige gegevens
CVE-2026-32162	8,40	Verkrijgen van verhoogde rechten

Input-Output Memory Management Unit (IOMMU):

CVE-ID	CVSS	Impact
CVE-2023-20585	5,30	<Vertaal: Tampering>

Universal Plug and Play (upnp.dll):

CVE-ID	CVSS	Impact
CVE-2026-32212	5,50	Toegang tot gevoelige gegevens
CVE-2026-32214	5,50	Toegang tot gevoelige gegevens

Windows Redirected Drive Buffering:

CVE-ID	CVSS	Impact
CVE-2026-32216	7,80	Verkrijgen van verhoogde rechten

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
CVE-2026-23670	5,70	Omzeilen van beveiligingsmaatregel
CVE-2026-32220	4,40	Omzeilen van beveiligingsmaatregel

Windows Active Directory:

CVE-ID	CVSS	Impact
CVE-2026-33826	8,00	Uitvoeren van willekeurige code
CVE-2026-32072	6,20	Voordoen als andere gebruiker

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2026-26165	7,00	Verkrijgen van verhoogde rechten
CVE-2026-26166	7,00	Verkrijgen van verhoogde rechten
CVE-2026-27918	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32202	4,30	Voordoen als andere gebruiker
CVE-2026-32151	6,50	Toegang tot gevoelige gegevens
CVE-2026-32225	8,80	Omzeilen van beveiligingsmaatregel

Windows Server Update Service:

CVE-ID	CVSS	Impact
CVE-2026-26154	7,50	<Vertaal: Tampering>
CVE-2026-26174	7,00	Verkrijgen van verhoogde rechten
CVE-2026-32224	7,00	Verkrijgen van verhoogde rechten

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2026-27921	7,00	Verkrijgen van verhoogde rechten

| CVE-2026-33827 | 8,10 | Uitvoeren van willekeurige code |

Windows Kernel Memory:

CVE-ID	CVSS	Impact
CVE-2026-26169	6,10	Toegang tot gevoelige gegevens

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2026-27913	7,70	Omzeilen van beveiligingsmaatregel

Windows GDI:

CVE-ID	CVSS	Impact
CVE-2026-27931	5,50	Toegang tot gevoelige gegevens
CVE-2026-27930	5,50	Toegang tot gevoelige gegevens

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2026-27912	8,00	Verkrijgen van verhoogde rechten

Windows RPC API:

CVE-ID	CVSS	Impact
CVE-2026-26183	7,80	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2026-32073	7,00	Verkrijgen van verhoogde rechten
CVE-2026-26168	7,80	Verkrijgen van verhoogde rechten
CVE-2026-26173	7,00	Verkrijgen van verhoogde rechten
CVE-2026-26177	7,00	Verkrijgen van verhoogde rechten
CVE-2026-26182	7,00	Verkrijgen van verhoogde rechten
CVE-2026-27922	7,00	Verkrijgen van verhoogde rechten
CVE-2026-33099	7,00	Verkrijgen van verhoogde rechten
CVE-2026-33100	7,00	Verkrijgen van verhoogde rechten

Windows Remote Desktop Licensing Service:

CVE-ID	CVSS	Impact
CVE-2026-26160	7,80	Verkrijgen van verhoogde rechten
CVE-2026-26159	7,80	Verkrijgen van verhoogde rechten

Windows Snipping Tool:

CVE-ID	CVSS	Impact
CVE-2026-32183	7,80	Uitvoeren van willekeurige code
CVE-2026-33829	4,30	Voordoen als andere gebruiker

Windows Local Security Authority Subsystem Service (LSASS):

CVE-ID	CVSS	Impact
CVE-2026-26155	6,50	Toegang tot gevoelige gegevens
CVE-2026-32071	7,50	Denial-of-Service

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2026-26152	7,00	Verkrijgen van verhoogde rechten

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

Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys):

CVE-ID	CVSS	Impact
CVE-2026-27917	7,00	Verkrijgen van verhoogde rechten

Windows Print Spooler Components:

CVE-ID	CVSS	Impact
CVE-2026-33101	7,80	Verkrijgen van verhoogde rechten

Windows Projected File System:

CVE-ID	CVSS	Impact
CVE-2026-27927	7,80	Verkrijgen van verhoogde rechten
CVE-2026-26184	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32069	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32074	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32078	7,80	Verkrijgen van verhoogde rechten

Windows LUAFV:

CVE-ID	CVSS	Impact
CVE-2026-27929	7,00	Verkrijgen van verhoogde rechten

Windows Universal Plug and Play (UPnP) Device Host:

CVE-ID	CVSS	Impact
CVE-2026-27915	7,80	Verkrijgen van verhoogde rechten
CVE-2026-27919	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32075	7,80	Verkrijgen van verhoogde rechten

CVE-2026-32156	8,40	Uitvoeren van willekeurige code
CVE-2026-27916	7,80	Verkrijgen van verhoogde rechten
CVE-2026-27920	7,80	Verkrijgen van verhoogde rechten
CVE-2026-27925	7,50	Toegang tot gevoelige gegevens
CVE-2026-32077	7,80	Verkrijgen van verhoogde rechten

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2026-33104	7,00	Verkrijgen van verhoogde rechten

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2026-27906	4,40	Omzeilen van beveiligingsmaatregel
CVE-2026-27928	7,70	Omzeilen van beveiligingsmaatregel

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-27926	7,00	Verkrijgen van verhoogde rechten

Windows Admin Center:

CVE-ID	CVSS	Impact
CVE-2026-32196	6,10	Voordoen als andere gebruiker

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2026-32222	7,80	Verkrijgen van verhoogde rechten

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

Remote Desktop Client:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-32157	8,80	Uitvoeren van willekeurige code

Windows WalletService:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-32080	7,00	Verkrijgen van verhoogde rechten

Microsoft Windows Search Component:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-27909	7,80	Verkrijgen van verhoogde rechten

Desktop Window Manager:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-27924	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32152	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32154	7,80	Verkrijgen van verhoogde rechten
CVE-2026-27923	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32155	7,80	Verkrijgen van verhoogde rechten

Windows HTTP.sys:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-33096	7,50	Denial-of-Service

Windows Secure Boot:

CVE-ID	CVSS	Impact
CVE-2026-25250	6,00	Omzeilen van beveiligingsmaatregel,

Microsoft PowerShell:

CVE-ID	CVSS	Impact
CVE-2026-26170	7,80	Verkrijgen van verhoogde rechten

Microsoft Windows:

CVE-ID	CVSS	Impact
CVE-2026-32181	5,50	Denial-of-Service

Windows SSDP Service:

CVE-ID	CVSS	Impact
CVE-2026-32082	7,00	Verkrijgen van verhoogde rechten
CVE-2026-32083	7,00	Verkrijgen van verhoogde rechten
CVE-2026-32068	7,00	Verkrijgen van verhoogde rechten

Windows Client Side Caching driver (csc.sys):

CVE-ID	CVSS	Impact
CVE-2026-26176	7,80	Verkrijgen van verhoogde rechten

Windows Sensor Data Service:

CVE-ID	CVSS	Impact

| CVE-2026-26161 | 7,80 | Verkrijgen van verhoogde rechten |

Windows Encrypting File System (EFS):

CVE-ID	CVSS	Impact
CVE-2026-26153	7,80	Verkrijgen van verhoogde rechten

Windows TDI Translation Driver (tdx.sys):

CVE-ID	CVSS	Impact
CVE-2026-27908	7,00	Verkrijgen van verhoogde rechten

Windows Storage Spaces Controller:

CVE-ID	CVSS	Impact
CVE-2026-27907	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32076	7,80	Verkrijgen van verhoogde rechten

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2026-26181	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32219	7,00	Verkrijgen van verhoogde rechten
CVE-2026-32091	7,80	Verkrijgen van verhoogde rechten

Windows IKE Extension:

CVE-ID	CVSS	Impact
CVE-2026-33824	9,80	Uitvoeren van willekeurige code

Windows Biometric Service:

CVE-ID	CVSS	Impact
CVE-2026-32088	6,10	Omzeilen van beveiligingsmaatregel

Windows Advanced Rasterization Platform:

CVE-ID	CVSS	Impact
CVE-2026-26178	8,80	Verkrijgen van verhoogde rechten

Windows OLE:

CVE-ID	CVSS	Impact
CVE-2026-26162	7,80	Verkrijgen van verhoogde rechten

Windows Recovery Environment Agent:

CVE-ID	CVSS	Impact
CVE-2026-20928	4,60	Omzeilen van beveiligingsmaatregel

Windows Speech Brokered Api:

CVE-ID	CVSS	Impact
CVE-2026-32089	7,80	Verkrijgen van verhoogde rechten
CVE-2026-32090	7,80	Verkrijgen van verhoogde rechten

Windows Container Isolation FS Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-33098	7,80	Verkrijgen van verhoogde rechten

```
|----------------|------|-------------------------------------|

Windows Management Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-20930 | 7,80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Role: Windows Hyper-V:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-26156 | 7,80 | Uitvoeren van willekeurige code     |
| CVE-2026-32149 | 7,30 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Windows Remote Desktop:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-26151 | 7,10 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|

Microsoft Graphics Component:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-32221 | 8,40 | 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-2026-32068	7.0 HIGH
CVE-2026-32069	7.8 HIGH
CVE-2026-32070	7.0 HIGH
CVE-2026-32071	7.5 HIGH
CVE-2026-32072	6.2 MEDIUM
CVE-2026-32073	7.0 HIGH
CVE-2026-32074	7.8 HIGH
CVE-2026-32075	7.0 HIGH
CVE-2026-32076	7.8 HIGH
CVE-2026-32077	7.8 HIGH
CVE-2026-32078	7.8 HIGH
CVE-2026-32079	5.5 MEDIUM
CVE-2026-32080	7.0 HIGH
CVE-2026-32081	5.5 MEDIUM
CVE-2026-32082	7.0 HIGH
CVE-2026-32083	7.0 HIGH
CVE-2026-32084	5.5 MEDIUM
CVE-2026-32085	5.5 MEDIUM
CVE-2026-32086	7.0 HIGH
CVE-2026-32087	7.0 HIGH
CVE-2026-32088	6.1 MEDIUM

CVE-2026-32089	7.8 HIGH
CVE-2026-32090	7.8 HIGH
CVE-2026-32091	8.4 HIGH
CVE-2026-32093	7.0 HIGH
CVE-2026-32149	7.3 HIGH
CVE-2026-32150	7.0 HIGH
CVE-2026-32151	6.5 MEDIUM
CVE-2026-32152	7.8 HIGH
CVE-2026-32153	7.8 HIGH
CVE-2026-32154	7.8 HIGH
CVE-2026-32155	7.8 HIGH
CVE-2026-32156	7.4 HIGH
CVE-2026-32157	8.8 HIGH
CVE-2026-32158	7.8 HIGH
CVE-2026-32159	7.8 HIGH
CVE-2026-32160	7.8 HIGH
CVE-2026-32162	8.4 HIGH
CVE-2026-32163	7.8 HIGH
CVE-2026-32164	7.8 HIGH
CVE-2026-32165	7.8 HIGH
CVE-2026-32181	5.5 MEDIUM
CVE-2026-32183	7.8 HIGH
CVE-2026-32195	7.0 HIGH

CVE-2026-32196	6.1 MEDIUM
CVE-2026-32202	4.3 MEDIUM
CVE-2026-32212	5.5 MEDIUM
CVE-2026-32214	5.5 MEDIUM
CVE-2026-32215	5.5 MEDIUM
CVE-2026-32216	5.5 MEDIUM
CVE-2026-32217	5.5 MEDIUM
CVE-2026-32218	5.5 MEDIUM
CVE-2026-32219	7.0 HIGH
CVE-2026-32220	4.4 MEDIUM
CVE-2026-32221	8.4 HIGH
CVE-2026-32222	7.8 HIGH
CVE-2026-32223	6.8 MEDIUM
CVE-2026-32224	7.0 HIGH
CVE-2026-32225	8.8 HIGH
CVE-2026-33096	7.5 HIGH
CVE-2026-33098	7.8 HIGH
CVE-2026-33099	7.0 HIGH
CVE-2026-33100	7.0 HIGH
CVE-2026-33101	7.8 HIGH
CVE-2026-33104	7.0 HIGH
CVE-2026-33824	9.8 CRITICAL
CVE-2026-33826	8.0 HIGH

CVE-2026-33827	8.1 HIGH
CVE-2026-33829	4.3 MEDIUM
CVE-2023-20585	5.3 MEDIUM
CVE-2026-0390	6.7 MEDIUM
CVE-2026-20806	5.5 MEDIUM
CVE-2026-20928	4.6 MEDIUM
CVE-2026-20930	7.8 HIGH
CVE-2026-23670	5.7 MEDIUM
CVE-2026-25184	7.0 HIGH
CVE-2026-25250	6.0 MEDIUM
CVE-2026-26151	7.1 HIGH
CVE-2026-26152	7.0 HIGH
CVE-2026-26153	7.8 HIGH
CVE-2026-26154	7.5 HIGH
CVE-2026-26155	6.5 MEDIUM
CVE-2026-26156	7.8 HIGH
CVE-2026-26159	7.8 HIGH
CVE-2026-26160	7.8 HIGH
CVE-2026-26161	7.8 HIGH
CVE-2026-26162	7.8 HIGH
CVE-2026-26163	7.8 HIGH
CVE-2026-26165	7.0 HIGH
CVE-2026-26166	7.0 HIGH

CVE-2026-26167	8.8 HIGH
CVE-2026-26168	7.8 HIGH
CVE-2026-26169	6.1 MEDIUM
CVE-2026-26170	7.8 HIGH
CVE-2026-26172	7.8 HIGH
CVE-2026-26173	7.0 HIGH
CVE-2026-26174	7.0 HIGH
CVE-2026-26175	4.6 MEDIUM
CVE-2026-26176	7.8 HIGH
CVE-2026-26177	7.0 HIGH
CVE-2026-26178	8.8 HIGH
CVE-2026-26179	7.8 HIGH
CVE-2026-26180	7.8 HIGH
CVE-2026-26181	7.8 HIGH
CVE-2026-26182	7.0 HIGH
CVE-2026-26183	7.8 HIGH
CVE-2026-26184	7.8 HIGH
CVE-2026-27906	4.4 MEDIUM
CVE-2026-27907	7.8 HIGH
CVE-2026-27908	7.0 HIGH
CVE-2026-27909	7.8 HIGH
CVE-2026-27910	7.8 HIGH
CVE-2026-27911	7.8 HIGH

CVE-2026-27912	8.0 HIGH
CVE-2026-27913	7.7 HIGH
CVE-2026-27914	7.8 HIGH
CVE-2026-27915	7.8 HIGH
CVE-2026-27916	7.8 HIGH
CVE-2026-27917	7.0 HIGH
CVE-2026-27918	7.8 HIGH
CVE-2026-27919	7.8 HIGH
CVE-2026-27920	7.8 HIGH
CVE-2026-27921	7.0 HIGH
CVE-2026-27922	7.0 HIGH
CVE-2026-27923	7.8 HIGH
CVE-2026-27924	7.8 HIGH
CVE-2026-27925	6.5 MEDIUM
CVE-2026-27926	7.0 HIGH
CVE-2026-27927	7.8 HIGH
CVE-2026-27928	8.7 HIGH
CVE-2026-27929	7.0 HIGH
CVE-2026-27930	5.5 MEDIUM
CVE-2026-27931	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
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-191	Integer Underflow (Wrap or Wraparound)
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-269	Improper Privilege Management
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-287	Improper Authentication
CWE-306	Missing Authentication for Critical Function
CWE-325	Missing Cryptographic Step
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-357	Insufficient UI Warning of Dangerous Operations
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-532	Insertion of Sensitive Information into Log File
CWE-681	Incorrect Conversion between Numeric Types
CWE-693	Protection Mechanism Failure
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-908	Use of Uninitialized Resource
CWE-922	Insecure Storage of Sensitive Information

Getroffen producten

Microsoft
Microsoft Windows 11 Version 26H1
Microsoft Windows Admin Center
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2016
Microsoft Windows Server 2019

Microsoft Windows Server 2022
Microsoft Windows Server 2025
Remote Desktop client for Windows Desktop
Windows
Windows 10
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
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 ARM systems
Windows 11 Version 25H2 for x64-based Systems
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 Admin Center
Windows App Client for Windows Desktop
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 Version 23H2
Windows Server 2022, 23H2 Edition (Server Core installation)
Windows Server 2025
Windows Server 2025 (Server Core installation)
Windows_11_25H2
window_server
windows_10
windows_11
windows_server_2012
windows_server_2016
windows_server_2016_(server_core_installation)
windows_server_2019
windows_server_2019_(server_core_installation)
windows_server_2022
windows_server_2025
windows_service_2012_server_core_installation

Disclaimer