Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0181

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 09-06-2026

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 een groot aantal kwetsbaarheden verholpen in Windows.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot diverse categorieën schade, zoals omschreven in onderstaande tabellen.

Tussen deze kwetsbaarheden zitten een zestal zeer ernstige, welke door Microsoft zijn ingeschaald met een CVSS score van 9 en hoger. Deze kwetsbaarheden bevinden zich in diverse componenten van Windows die bereikbaar en benaderbaar zijn vanaf netwerkverbindingen, zoals http.sys, DHCP, de Kernel en TCP/IP. Door de externe bereikbaarheid en de mogelijkheden tot uitvoer van willekeurige code, is het risico op grootschalig misbruik op korte termijn aanwezig. Op dit moment wordt (nog) geen actief misbruik waargenomen en is (nog) geen publieke Proof-of-Concept (PoC) of exploit bekend, maar het NCSC verwacht deze wel op korte termijn en adviseert daarom deze updates met spoed in te zetten.

```
Windows TCP/IP:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-42904 | 9.60 | Verkrijgen van verhoogde rechten    |
| CVE-2026-42915 | 5.70 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows BitLocker:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45655 | 5.30 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-45658 | 7.80 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-50507 | 6.80 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|

Windows Mark of the Web (MOTW):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45595 | 5.40 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|
```

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2026-44803	7.80	Uitvoeren van willekeurige code
CVE-2026-44812	7.80	Uitvoeren van willekeurige code

Windows Push Notifications:

CVE-ID	CVSS	Impact
CVE-2026-42969	5.50	Toegang tot gevoelige gegevens
CVE-2026-42971	5.50	Toegang tot gevoelige gegevens
CVE-2026-42970	5.50	Toegang tot gevoelige gegevens
CVE-2026-42973	5.50	Toegang tot gevoelige gegevens
CVE-2026-42978	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42977	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42979	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42991	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows DNS:

CVE-ID	CVSS	Impact
CVE-2026-41108	7.00	Verkrijgen van verhoogde rechten

Windows Bluetooth Port Driver:

CVE-ID	CVSS	Impact
CVE-2026-45640	7.00	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2026-34335	7.00	Verkrijgen van verhoogde rechten

```
| CVE-2026-45601 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45598 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45596 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45638 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45603 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-42911 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Function Discovery Service (fdwsd.dll):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-42836 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Kernel:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-10263 | 9.30 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45657 | 9.80 | Uitvoeren van willekeurige code     |
| CVE-2026-48583 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45653 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-42984 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Secure Boot:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45588 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48568 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48570 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48573 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48575 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48576 | 7.90 | Omzeilen van beveiligingsmaatregel  |
| CVE-2026-48578 | 7.90 | Verkrijgen van verhoogde rechten    |
| CVE-2026-45654 | 7.90 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|

Remote Desktop Client:
```

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-47289 | 8.80 | Uitvoeren van willekeurige code     |
| CVE-2026-47653 | 8.80 | Uitvoeren van willekeurige code     |
| CVE-2026-47654 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-48563 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-42909 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-42913 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-42992 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-44799 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-44801 | 7.50 | Uitvoeren van willekeurige code     |
| CVE-2026-42985 | 8.80 | Uitvoeren van willekeurige code     |
| CVE-2026-42993 | 7.50 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Microsoft UxTheme Library (uxtheme.dll):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45606 | 5.50 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows Kernel-Mode Drivers:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45600 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows DHCP Client:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45608 | 6.80 | Toegang tot gevoelige gegevens      |
| CVE-2026-44815 | 9.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Universal Plug and Play (upnp.dll):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

CVE-2026-45599	8.10	Uitvoeren van willekeurige code
CVE-2026-45635	8.10	Uitvoeren van willekeurige code

Windows Bluetooth Service:

CVE-ID	CVSS	Impact
CVE-2026-45605	7.80	Verkrijgen van verhoogde rechten

Windows UEFI:

CVE-ID	CVSS	Impact
CVE-2026-45656	7.80	Omzeilen van beveiligingsmaatregel
CVE-2026-8863	7.80	Omzeilen van beveiligingsmaatregel

Windows Hotpatch Monitoring Service:

CVE-ID	CVSS	Impact
CVE-2026-42910	7.80	Verkrijgen van verhoogde rechten

Microsoft Azure Attestation service and Device Health Attestation Service:

CVE-ID	CVSS	Impact
CVE-2026-33828	7.80	Verkrijgen van verhoogde rechten
CVE-2026-45642	3.90	Voordoen als andere gebruiker

Windows RDP:

CVE-ID	CVSS	Impact
CVE-2026-45639	7.50	Toegang tot gevoelige gegevens
CVE-2026-42908	7.50	Toegang tot gevoelige gegevens

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

Winlogon:

CVE-ID	CVSS	Impact
CVE-2026-42989	7.80	Verkrijgen van verhoogde rechten

Windows Collaborative Translation Framework:

CVE-ID	CVSS	Impact
CVE-2026-45586	7.80	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2026-47288	7.10	Uitvoeren van willekeurige code
CVE-2026-42903	6.50	Denial-of-Service
CVE-2026-42914	5.30	Denial-of-Service

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2026-44810	8.40	Verkrijgen van verhoogde rechten

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2026-45636	7.80	Uitvoeren van willekeurige code

Windows Universal Disk Format File System Driver (UDFS):

CVE-ID	CVSS	Impact
CVE-2026-40409	7.80	Verkrijgen van verhoogde rechten
CVE-2026-40404	7.80	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2026-42986	7.80	Verkrijgen van verhoogde rechten

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2026-45607	8.40	Uitvoeren van willekeurige code
CVE-2026-47652	8.20	Uitvoeren van willekeurige code

Windows NT OS Kernel:

CVE-ID	CVSS	Impact
CVE-2026-42980	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42916	7.80	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2026-44809	7.80	Verkrijgen van verhoogde rechten

Windows Projected File System Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-42828	7.80	Verkrijgen van verhoogde rechten

```
| CVE-2026-42837 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

UI Automation Manager (uiamanager.dll):

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45597 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows HTTP.sys:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-47291 | 9.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

Microsoft Kinect:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-41092 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows SDK:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45593 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows Media:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-48574 | 7.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

Windows Performance Monitor:

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

CVE-2026-42981	8.10	Uitvoeren van willekeurige code
CVE-2026-42974	8.10	Uitvoeren van willekeurige code

Windows Application Identity (AppID) Subsystem:

CVE-ID	CVSS	Impact
CVE-2026-45594	5.50	Toegang tot gevoelige gegevens
CVE-2026-45604	5.50	Toegang tot gevoelige gegevens

Windows Administrator Protection:

CVE-ID	CVSS	Impact
CVE-2026-42829	7.80	Omzeilen van beveiligingsmaatregel

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2026-45641	8.40	Uitvoeren van willekeurige code
CVE-2026-42972	5.50	Toegang tot gevoelige gegevens

Windows Narrator Braille:

CVE-ID	CVSS	Impact
CVE-2026-48565	7.80	Verkrijgen van verhoogde rechten

Windows DHCP Server:

CVE-ID	CVSS	Impact
CVE-2026-45634	5.50	Toegang tot gevoelige gegevens
CVE-2026-45602	9.10	Manipulatie van gegevens

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

Windows Internet (wininet.dll):

CVE-ID	CVSS	Impact
CVE-2026-45592	7.80	Verkrijgen van verhoogde rechten

Windows Deployment Services:

CVE-ID	CVSS	Impact
CVE-2026-42987	8.10	Uitvoeren van willekeurige code

HTTP/2:

CVE-ID	CVSS	Impact
CVE-2026-49160	7.50	Denial-of-Service

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2026-42912	7.00	Verkrijgen van verhoogde rechten
CVE-2026-42968	5.50	Toegang tot gevoelige gegevens

Windows Network Controller (NC) Host Agent:

CVE-ID	CVSS	Impact
CVE-2026-44805	5.50	Denial-of-Service

Windows DWM Core Library:

| CVE-ID | CVSS | Impact |

CVE-2026-48566	5.50	Toegang tot gevoelige gegevens
CVE-2026-45637	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42905	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44811	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44808	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44807	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42983	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44802	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44814	5.50	Toegang tot gevoelige gegevens
CVE-2026-44813	7.80	Verkrijgen van verhoogde rechten
CVE-2026-44804	7.80	Verkrijgen van verhoogde rechten

Windows Boot Manager:

CVE-ID	CVSS	Impact
CVE-2026-47656	7.90	Omzeilen van beveiligingsmaatregel

Windows Program Compatibility Assistant Service:

CVE-ID	CVSS	Impact
CVE-2026-45487	7.80	Verkrijgen van verhoogde rechten

Windows Storage:

CVE-ID	CVSS	Impact
CVE-2026-47648	7.00	Verkrijgen van verhoogde rechten

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2026-42906	5.50	Toegang tot gevoelige gegevens
CVE-2026-42907	6.50	Toegang tot gevoelige gegevens

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

Active Directory Domain Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-45648 | 8.80 | 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-2025-10263	5.1 MEDIUM
CVE-2026-33828	7.8 HIGH
CVE-2026-34335	7.0 HIGH
CVE-2026-40404	7.8 HIGH
CVE-2026-40409	7.8 HIGH
CVE-2026-41092	7.8 HIGH
CVE-2026-41108	7.0 HIGH
CVE-2026-42828	7.8 HIGH
CVE-2026-42829	7.8 HIGH
CVE-2026-42836	7.0 HIGH
CVE-2026-42837	7.8 HIGH

CVE-2026-42903	6.5 MEDIUM
CVE-2026-42904	9.6 CRITICAL
CVE-2026-42905	7.8 HIGH
CVE-2026-42906	5.5 MEDIUM
CVE-2026-42907	6.5 MEDIUM
CVE-2026-42908	7.5 HIGH
CVE-2026-42909	7.5 HIGH
CVE-2026-42910	7.8 HIGH
CVE-2026-42911	7.0 HIGH
CVE-2026-42912	7.0 HIGH
CVE-2026-42913	7.5 HIGH
CVE-2026-42914	5.3 MEDIUM
CVE-2026-42915	5.7 MEDIUM
CVE-2026-42916	7.8 HIGH
CVE-2026-42968	5.5 MEDIUM
CVE-2026-42969	5.5 MEDIUM
CVE-2026-42970	5.5 MEDIUM
CVE-2026-42971	5.5 MEDIUM
CVE-2026-42972	5.5 MEDIUM
CVE-2026-42973	5.5 MEDIUM
CVE-2026-42974	8.1 HIGH
CVE-2026-42977	7.8 HIGH
CVE-2026-42978	7.8 HIGH

CVE-2026-42979	7.8 HIGH
CVE-2026-42980	7.8 HIGH
CVE-2026-42981	8.1 HIGH
CVE-2026-42983	7.8 HIGH
CVE-2026-42984	7.0 HIGH
CVE-2026-42985	8.8 HIGH
CVE-2026-42986	7.8 HIGH
CVE-2026-42987	8.1 HIGH
CVE-2026-42989	7.8 HIGH
CVE-2026-42991	7.8 HIGH
CVE-2026-42992	7.5 HIGH
CVE-2026-42993	7.5 HIGH
CVE-2026-44799	7.5 HIGH
CVE-2026-44801	7.5 HIGH
CVE-2026-44802	7.8 HIGH
CVE-2026-44803	7.8 HIGH
CVE-2026-44804	7.8 HIGH
CVE-2026-44805	5.5 MEDIUM
CVE-2026-44807	7.8 HIGH
CVE-2026-44808	7.8 HIGH
CVE-2026-44809	7.8 HIGH
CVE-2026-44810	8.4 HIGH
CVE-2026-44811	7.8 HIGH

CVE-2026-44812	7.8 HIGH
CVE-2026-44813	7.8 HIGH
CVE-2026-44814	5.5 MEDIUM
CVE-2026-44815	9.8 CRITICAL
CVE-2026-45487	7.8 HIGH
CVE-2026-45586	7.8 HIGH
CVE-2026-45588	7.9 HIGH
CVE-2026-45592	7.8 HIGH
CVE-2026-45593	7.8 HIGH
CVE-2026-45594	5.5 MEDIUM
CVE-2026-45595	5.4 MEDIUM
CVE-2026-45596	7.0 HIGH
CVE-2026-45597	7.0 HIGH
CVE-2026-45598	7.0 HIGH
CVE-2026-45599	8.1 HIGH
CVE-2026-45600	7.8 HIGH
CVE-2026-45601	7.0 HIGH
CVE-2026-45602	9.1 CRITICAL
CVE-2026-45603	7.0 HIGH
CVE-2026-45604	5.5 MEDIUM
CVE-2026-45605	7.8 HIGH
CVE-2026-45606	5.5 MEDIUM
CVE-2026-45607	8.4 HIGH

CVE-2026-45608	6.8 MEDIUM
CVE-2026-45634	5.5 MEDIUM
CVE-2026-45635	8.1 HIGH
CVE-2026-45636	7.8 HIGH
CVE-2026-45637	7.8 HIGH
CVE-2026-45638	7.8 HIGH
CVE-2026-45639	7.5 HIGH
CVE-2026-45640	7.0 HIGH
CVE-2026-45641	8.4 HIGH
CVE-2026-45642	3.9 LOW
CVE-2026-45648	8.8 HIGH
CVE-2026-45653	7.0 HIGH
CVE-2026-45654	7.9 HIGH
CVE-2026-45655	5.3 MEDIUM
CVE-2026-45656	7.8 HIGH
CVE-2026-45657	9.8 CRITICAL
CVE-2026-45658	7.8 HIGH
CVE-2026-47288	7.1 HIGH
CVE-2026-47289	8.8 HIGH
CVE-2026-47291	9.8 CRITICAL
CVE-2026-47648	7.0 HIGH
CVE-2026-47652	8.2 HIGH
CVE-2026-47653	8.8 HIGH

CVE-2026-47654	7.5 HIGH
CVE-2026-47656	7.9 HIGH
CVE-2026-48563	7.5 HIGH
CVE-2026-48565	7.8 HIGH
CVE-2026-48566	5.5 MEDIUM
CVE-2026-48568	7.9 HIGH
CVE-2026-48570	7.9 HIGH
CVE-2026-48573	7.9 HIGH
CVE-2026-48574	7.8 HIGH
CVE-2026-48575	7.9 HIGH
CVE-2026-48576	7.9 HIGH
CVE-2026-48578	7.9 HIGH
CVE-2026-48583	7.8 HIGH
CVE-2026-49160	7.5 HIGH
CVE-2026-50507	6.8 MEDIUM
CVE-2026-8863	

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-121	Stack-based Buffer Overflow

CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-131	Incorrect Calculation of Buffer Size
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-197	Numeric Truncation Error
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-306	Missing Authentication for Critical Function
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-400	Uncontrolled Resource Consumption
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-476	NULL Pointer Dereference
CWE-501	Trust Boundary Violation
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')
CWE-908	Use of Uninitialized Resource

CWE-1329	Reliance on Component That is Not Updateable

Getroffen producten

Microsoft
Microsoft Windows 11
Microsoft Windows 11 Version 26H1
Microsoft Windows Server 2025
Windows 10
Windows 10 1803
Windows 10 1809
Windows 10 1903
Windows 10 1909
Windows 10 2004
Windows 10 20h2
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64- based Systems
Windows 10 Version 1803

Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1809
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1909
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004
Windows 10 Version 2004 for 32-bit Systems

Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 20H2
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-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 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 for ARM64-based Systems
Windows 11 Version 26H1 for x64-based Systems
Windows 11 version 26H1
Windows 11 version 26H1 for x64-based Systems
Windows Narrator Braille
Windows Server
Windows Server 1903
Windows Server 1909
Windows Server 2004
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 2025
Windows Server 2025 (Server Core installation)
Windows Server 20H2
Windows Server version 2004
Windows Server version 20H2
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.