Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0284

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-08-2026

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 de categorieën schade, zoals genoemd in onderstaande tabel.

De ernstigste kwetsbaarheden hebben kenmerken **CVE-2026-59124, CVE-2026-62815, CVE-2026-62878, CVE-2026-62893** en **CVE-2026-65791** toegewezen gekregen en bevinden zich in respectievelijk Telephony Service, QUIC, DNS Server, Capability Access Management Service en iSCSI Target Service. Kwaadwillenden met toegang tot deze services kunnen zonder voorafgaande authenticatie mogelijk code uitvoeren of zich toegang verschaffen tot het kwetsbare systeem.

Naast deze ernstige kwetsbaarheden zijn nog eens meer dan 230 kwetsbaarheden verholpen, allen varierend in ernstigheid van middelmatig tot hoog/kritiek.

Door de aard en omvang van deze updates, adviseert het NCSC om deze updates met voorrang in te zetten.

```
Windows Accessibility Infrastructure (ATBroker.exe):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-61358 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Kernel:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-54113 | 7.50 | Denial-of-Service                   |
| CVE-2026-61930 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62737 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-61929 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62708 | 6.40 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62749 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62780 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62788 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2026-65773 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2026-61928	5.50	Manipulatie van gegevens

Windows Schannel:

CVE-ID	CVSS	Impact
CVE-2026-62779	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62757	5.30	Omzeilen van beveiligingsmaatregel

AMD Zen:

CVE-ID	CVSS	Impact
CVE-2026-59130	5.60	Toegang tot gevoelige gegevens
CVE-2026-59131	5.60	Toegang tot gevoelige gegevens

Windows Secure Socket Tunneling Protocol (SSTP):

CVE-ID	CVSS	Impact
CVE-2026-62889	8.10	Uitvoeren van willekeurige code

Windows Remote Access API:

CVE-ID	CVSS	Impact
CVE-2026-65671	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65672	7.80	Verkrijgen van verhoogde rechten

Windows Win32K:

CVE-ID	CVSS	Impact

CVE-2026-62712	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62746	5.50	Toegang tot gevoelige gegevens
CVE-2026-62798	5.50	Toegang tot gevoelige gegevens
CVE-2026-62876	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62877	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65678	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62711	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62733	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62743	5.50	Toegang tot gevoelige gegevens
CVE-2026-62786	5.50	Toegang tot gevoelige gegevens
CVE-2026-62885	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65775	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65776	7.00	Verkrijgen van verhoogde rechten

Windows Autopilot:

CVE-ID	CVSS	Impact
CVE-2026-65783	7.00	Verkrijgen van verhoogde rechten
CVE-2026-65779	7.00	Verkrijgen van verhoogde rechten
CVE-2026-65780	7.00	Verkrijgen van verhoogde rechten
CVE-2026-65778	7.00	Verkrijgen van verhoogde rechten
CVE-2026-65782	7.00	Verkrijgen van verhoogde rechten
CVE-2026-65781	7.00	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2026-62819	8.10	Uitvoeren van willekeurige code

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2026-62728	7.00	Verkrijgen van verhoogde rechten

Windows Remote Desktop Services:

CVE-ID	CVSS	Impact
CVE-2026-61356	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61367	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62692	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61364	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61365	7.80	Verkrijgen van verhoogde rechten

Microsoft QUIC:

CVE-ID	CVSS	Impact
CVE-2026-62815	9.80	Uitvoeren van willekeurige code

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2026-59127	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61925	7.80	Verkrijgen van verhoogde rechten
CVE-2026-70344	7.80	Verkrijgen van verhoogde rechten
CVE-2026-70345	7.80	Verkrijgen van verhoogde rechten
CVE-2026-70346	7.80	Verkrijgen van verhoogde rechten
CVE-2026-70347	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61938	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62768	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65774	7.80	Verkrijgen van verhoogde rechten

Windows Network Address Translation (NAT):

CVE-ID	CVSS	Impact
CVE-2026-56179	8.30	Voordoen als andere gebruiker

Windows Storage Port Driver:

CVE-ID	CVSS	Impact
CVE-2026-65814	7.80	Verkrijgen van verhoogde rechten

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2026-61350	4.60	Toegang tot gevoelige gegevens
CVE-2026-62796	5.50	Toegang tot gevoelige gegevens
CVE-2026-62797	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65784	5.50	Toegang tot gevoelige gegevens
CVE-2026-62700	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62793	5.50	Toegang tot gevoelige gegevens
CVE-2026-62880	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62887	5.50	Toegang tot gevoelige gegevens

User-Mode Power Service (UMPS):

CVE-ID	CVSS	Impact
CVE-2026-62721	7.80	Verkrijgen van verhoogde rechten

Windows Bind Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-61927	7.00	Verkrijgen van verhoogde rechten
CVE-2026-61934	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62705	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62722	7.80	Verkrijgen van verhoogde rechten

Virtual Hard Disk (VHD) Miniport Driver:

CVE-ID	CVSS	Impact

| CVE-2026-59125 | 7.00 | Verkrijgen van verhoogde rechten |

Windows Narrator Braille:

CVE-ID	CVSS	Impact
CVE-2026-56174	7.80	Verkrijgen van verhoogde rechten

Microsoft Remote Registry Service:

CVE-ID	CVSS	Impact
CVE-2026-59138	6.50	Denial-of-Service
CVE-2026-61345	6.50	Denial-of-Service

Windows Key Guard:

CVE-ID	CVSS	Impact
CVE-2026-66799	7.80	Verkrijgen van verhoogde rechten

Windows RPC API:

CVE-ID	CVSS	Impact
CVE-2026-42976	7.80	Verkrijgen van verhoogde rechten

Windows User Profile Service:

CVE-ID	CVSS	Impact
CVE-2026-62832	7.80	Verkrijgen van verhoogde rechten

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2026-61353	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62723	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62724	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62748	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62729	7.00	Verkrijgen van verhoogde rechten
CVE-2026-59122	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62701	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62725	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62726	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62732	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62734	7.00	Verkrijgen van verhoogde rechten

Capability Access Management Service (camsvc):

CVE-ID	CVSS	Impact
CVE-2026-62892	7.00	Verkrijgen van verhoogde rechten

Windows Imaging Component:

CVE-ID	CVSS	Impact
CVE-2026-54984	7.80	Uitvoeren van willekeurige code
CVE-2026-62740	5.50	Toegang tot gevoelige gegevens

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2026-62719	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62717	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65790	7.80	Verkrijgen van verhoogde rechten

Windows Defender Firewall Service:

CVE-ID	CVSS	Impact
CVE-2026-61936	5.50	Omzeilen van beveiligingsmaatregel

RPC Runtime:

CVE-ID	CVSS	Impact
CVE-2026-62781	8.10	Uitvoeren van willekeurige code

Windows Program Compatibility Assistant Service:

CVE-ID	CVSS	Impact
CVE-2026-62696	7.80	Verkrijgen van verhoogde rechten

Windows Active Directory:

CVE-ID	CVSS	Impact
CVE-2026-49179	8.80	Uitvoeren van willekeurige code
CVE-2026-65777	5.30	Omzeilen van beveiligingsmaatregel

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2026-62770	7.80	Verkrijgen van verhoogde rechten

Windows LUAFV:

CVE-ID	CVSS	Impact
CVE-2026-50472	7.00	Verkrijgen van verhoogde rechten

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2026-59132	7.50	Denial-of-Service
CVE-2026-62792	8.10	Uitvoeren van willekeurige code

Windows Device Association Service:

CVE-ID	CVSS	Impact
CVE-2026-62747	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62710	7.80	Verkrijgen van verhoogde rechten

Windows Storage:

CVE-ID	CVSS	Impact
CVE-2026-62695	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61359	7.80	Verkrijgen van verhoogde rechten

Windows GDI:

CVE-ID	CVSS	Impact
CVE-2026-65662	5.50	Toegang tot gevoelige gegevens
CVE-2026-61360	5.50	Toegang tot gevoelige gegevens

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2026-62754	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62766	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62773	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62752	7.80	Verkrijgen van verhoogde rechten

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

Windows Cross Device Service:

CVE-ID	CVSS	Impact
CVE-2026-66804	7.80	Verkrijgen van verhoogde rechten

Windows Deployment Services:

CVE-ID	CVSS	Impact
CVE-2026-62893	9.80	Uitvoeren van willekeurige code

Windows GDI+:

CVE-ID	CVSS	Impact
CVE-2026-62890	7.80	Uitvoeren van willekeurige code
CVE-2026-62709	5.50	Toegang tot gevoelige gegevens
CVE-2026-62822	8.80	Uitvoeren van willekeurige code

Windows iSCSI Target Service:

CVE-ID	CVSS	Impact
CVE-2026-65681	7.50	Denial-of-Service
CVE-2026-65679	8.10	Uitvoeren van willekeurige code
CVE-2026-65791	9.80	Uitvoeren van willekeurige code
CVE-2026-65796	5.90	Denial-of-Service

Windows Encrypting File System (EFS):

CVE-ID	CVSS	Impact
CVE-2026-59128	5.50	Toegang tot gevoelige gegevens

Application Information Services:

CVE-ID	CVSS	Impact
CVE-2026-61357	7.80	Verkrijgen van verhoogde rechten

Windows Container Isolation FS Filter Driver (unionfs.sys):

CVE-ID	CVSS	Impact
CVE-2026-62772	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62775	5.50	Toegang tot gevoelige gegevens

Microsoft Local Security Authority Server (lsasrv):

CVE-ID	CVSS	Impact
CVE-2026-62784	8.80	Uitvoeren van willekeurige code

Windows TPM:

CVE-ID	CVSS	Impact
CVE-2026-6727	5.90	Toegang tot gevoelige gegevens
CVE-2026-6726	7.90	Voordoen als andere gebruiker

Windows USB Driver:

CVE-ID	CVSS	Impact
CVE-2026-61926	7.80	Verkrijgen van verhoogde rechten

Windows Projected File System:

CVE-ID	CVSS	Impact

| CVE-2026-62751 | 7.80 | Verkrijgen van verhoogde rechten |

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2026-62785	8.80	Uitvoeren van willekeurige code
CVE-2026-62795	8.80	Uitvoeren van willekeurige code

Windows Universal Disk Format File System Driver (UDFS):

CVE-ID	CVSS	Impact
CVE-2026-62699	6.80	Uitvoeren van willekeurige code

Windows Backup Engine:

CVE-ID	CVSS	Impact
CVE-2026-62908	7.00	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2026-62713	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62771	7.80	Verkrijgen van verhoogde rechten

Windows Management Instrumentation:

CVE-ID	CVSS	Impact
CVE-2026-62738	5.50	Toegang tot gevoelige gegevens

Microsoft Azure Attestation service and Device Health Attestation Service:

CVE-ID	CVSS	Impact
CVE-2026-66802	8.10	Uitvoeren van willekeurige code
CVE-2026-71331	8.10	Uitvoeren van willekeurige code

Windows Push Notifications:

CVE-ID	CVSS	Impact
CVE-2026-62690	7.00	Verkrijgen van verhoogde rechten

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2026-59134	7.50	Uitvoeren van willekeurige code
CVE-2026-61924	6.50	Toegang tot gevoelige gegevens
CVE-2026-61352	7.50	Uitvoeren van willekeurige code
CVE-2026-61363	7.50	Uitvoeren van willekeurige code
CVE-2026-61918	6.50	Toegang tot gevoelige gegevens
CVE-2026-61921	6.50	Toegang tot gevoelige gegevens
CVE-2026-62824	8.80	Uitvoeren van willekeurige code

Microsoft High Performance Computing (HPC) Pack:

CVE-ID	CVSS	Impact
CVE-2026-59124	9.80	Uitvoeren van willekeurige code
CVE-2026-59133	8.80	Verkrijgen van verhoogde rechten

Microsoft Windows Search Component:

CVE-ID	CVSS	Impact
CVE-2026-59135	5.50	Toegang tot gevoelige gegevens

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

Desktop Window Manager:

CVE-ID	CVSS	Impact
CVE-2026-65786	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65787	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65788	7.00	Verkrijgen van verhoogde rechten

Windows SMB Client:

CVE-ID	CVSS	Impact
CVE-2026-62799	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62782	6.50	Toegang tot gevoelige gegevens
CVE-2026-65794	6.50	Toegang tot gevoelige gegevens

Windows DNS:

CVE-ID	CVSS	Impact
CVE-2026-62787	7.50	Uitvoeren van willekeurige code
CVE-2026-62817	8.80	Uitvoeren van willekeurige code
CVE-2026-62820	8.10	Uitvoeren van willekeurige code
CVE-2026-62878	9.80	Uitvoeren van willekeurige code
CVE-2026-65789	8.10	Uitvoeren van willekeurige code
CVE-2026-70304	6.70	Verkrijgen van verhoogde rechten
CVE-2026-70330	6.70	Verkrijgen van verhoogde rechten
CVE-2026-61920	6.60	Uitvoeren van willekeurige code
CVE-2026-62769	6.70	Verkrijgen van verhoogde rechten
CVE-2026-62778	8.10	Verkrijgen van verhoogde rechten
CVE-2026-62881	6.70	Verkrijgen van verhoogde rechten
CVE-2026-62883	6.70	Verkrijgen van verhoogde rechten
CVE-2026-65795	6.70	Verkrijgen van verhoogde rechten
CVE-2026-65797	6.70	Verkrijgen van verhoogde rechten
CVE-2026-65799	6.70	Verkrijgen van verhoogde rechten
CVE-2026-65798	6.70	Verkrijgen van verhoogde rechten

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

Windows Network File System:

CVE-ID	CVSS	Impact
CVE-2026-68819	5.90	Denial-of-Service

Windows HTTP.sys:

CVE-ID	CVSS	Impact
CVE-2026-61937	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62753	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62735	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62739	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62741	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62811	7.80	Verkrijgen van verhoogde rechten

Windows Display Enhancement Service:

CVE-ID	CVSS	Impact
CVE-2026-61923	7.80	Verkrijgen van verhoogde rechten

Windows SMB Server:

CVE-ID	CVSS	Impact
CVE-2026-62800	8.80	Uitvoeren van willekeurige code
CVE-2026-62790	8.80	Uitvoeren van willekeurige code

Reliable Multicast Transport Driver (RMCAST):

CVE-ID	CVSS	Impact
CVE-2026-62816	8.80	Uitvoeren van willekeurige code

Windows Management Services:

CVE-ID	CVSS	Impact
CVE-2026-70348	5.50	Denial-of-Service

Windows HTTP Protocol Stack:

CVE-ID	CVSS	Impact
CVE-2026-62750	6.50	Manipulatie van gegevens

Windows Graphics Kernel:

CVE-ID	CVSS	Impact
CVE-2026-61346	7.00	Verkrijgen van verhoogde rechten
CVE-2026-62702	6.80	Denial-of-Service
CVE-2026-62774	7.00	Verkrijgen van verhoogde rechten

Windows Event Logging Service:

CVE-ID	CVSS	Impact
CVE-2026-59137	5.50	Toegang tot gevoelige gegevens
CVE-2026-61347	5.50	Toegang tot gevoelige gegevens
CVE-2026-59126	7.00	Verkrijgen van verhoogde rechten

Windows Sensor Data Service:

CVE-ID	CVSS	Impact
CVE-2026-61355	7.80	Verkrijgen van verhoogde rechten

Winlogon:

CVE-ID	CVSS	Impact
CVE-2026-61939	7.00	Verkrijgen van verhoogde rechten

Windows Work Folder Service:

CVE-ID	CVSS	Impact
CVE-2026-61349	7.80	Verkrijgen van verhoogde rechten

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2026-61348	7.00	Verkrijgen van verhoogde rechten
CVE-2026-68820	7.00	Verkrijgen van verhoogde rechten
CVE-2026-70307	7.00	Verkrijgen van verhoogde rechten

Windows Modern Device Management (MDM):

CVE-ID	CVSS	Impact
CVE-2026-62707	7.80	Verkrijgen van verhoogde rechten

Microsoft COM for Windows:

CVE-ID	CVSS	Impact
CVE-2026-59136	5.50	Toegang tot gevoelige gegevens

Windows Network Connection Broker:

CVE-ID	CVSS	Impact
CVE-2026-61366	7.00	Verkrijgen van verhoogde rechten

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

Windows License Manager:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-62777	7.80	Verkrijgen van verhoogde rechten

Windows Wired AutoConfig Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-62730	5.50	Toegang tot gevoelige gegevens

Windows DWM Core Library:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-61932	7.80	Verkrijgen van verhoogde rechten
CVE-2026-61933	5.50	Toegang tot gevoelige gegevens
CVE-2026-62703	5.50	Toegang tot gevoelige gegevens
CVE-2026-62894	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62888	7.80	Verkrijgen van verhoogde rechten

Windows Hyper-V:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-61368	5.00	Toegang tot gevoelige gegevens

Microsoft Digest Authentication:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2026-62698	7.80	Verkrijgen van verhoogde rechten

Windows MIDI Service Module:

CVE-ID	CVSS	Impact
CVE-2026-62688	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62693	7.00	Verkrijgen van verhoogde rechten

Windows DHCP Client:

CVE-ID	CVSS	Impact
CVE-2026-61361	7.00	Uitvoeren van willekeurige code
CVE-2026-62755	7.80	Verkrijgen van verhoogde rechten
CVE-2026-65785	6.50	Denial-of-Service
CVE-2026-62736	7.80	Verkrijgen van verhoogde rechten

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact
CVE-2026-62783	7.80	Verkrijgen van verhoogde rechten
CVE-2026-62758	7.80	Verkrijgen van verhoogde rechten

Active Directory Certificate Services (AD CS):

CVE-ID	CVSS	Impact
CVE-2026-62818	8.80	Uitvoeren van willekeurige code

Windows DHCP Server:

CVE-ID	CVSS	Impact
CVE-2026-62718	6.50	Toegang tot gevoelige gegevens
CVE-2026-62715	6.50	Toegang tot gevoelige gegevens
CVE-2026-62716	6.50	Toegang tot gevoelige gegevens
CVE-2026-62742	6.50	Toegang tot gevoelige gegevens

```
| CVE-2026-62745 | 6.50 | Toegang tot gevoelige gegevens      |
| CVE-2026-62812 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62720 | 6.50 | Toegang tot gevoelige gegevens      |
| CVE-2026-62714 | 6.50 | Toegang tot gevoelige gegevens      |
| CVE-2026-62761 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62776 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62803 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62807 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2026-62814 | 6.50 | Toegang tot gevoelige gegevens      |
| CVE-2026-62823 | 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-2026-50472	7.0 HIGH
CVE-2026-56174	7.8 HIGH
CVE-2026-54113	7.5 HIGH
CVE-2026-54984	7.8 HIGH
CVE-2026-49179	8.8 HIGH
CVE-2026-6727	5.9 MEDIUM
CVE-2026-59127	7.8 HIGH
CVE-2026-59128	5.5 MEDIUM
CVE-2026-59130	5.6 MEDIUM

CVE-2026-59132	7.5 HIGH
CVE-2026-59135	5.5 MEDIUM
CVE-2026-59134	7.5 HIGH
CVE-2026-59136	5.5 MEDIUM
CVE-2026-59137	5.5 MEDIUM
CVE-2026-59138	6.5 MEDIUM
CVE-2026-61345	6.5 MEDIUM
CVE-2026-61346	7.0 HIGH
CVE-2026-61353	7.8 HIGH
CVE-2026-61347	5.5 MEDIUM
CVE-2026-61348	7.0 HIGH
CVE-2026-61350	4.6 MEDIUM
CVE-2026-61356	7.8 HIGH
CVE-2026-61367	7.8 HIGH
CVE-2026-61923	7.8 HIGH
CVE-2026-61366	7.0 HIGH
CVE-2026-61368	5.0 MEDIUM
CVE-2026-61924	6.5 MEDIUM
CVE-2026-61925	7.8 HIGH
CVE-2026-61928	5.5 MEDIUM
CVE-2026-61930	7.8 HIGH
CVE-2026-61937	7.8 HIGH
CVE-2026-62692	7.8 HIGH

CVE-2026-61932	7.8 HIGH
CVE-2026-61936	5.5 MEDIUM
CVE-2026-61939	7.0 HIGH
CVE-2026-62690	7.0 HIGH
CVE-2026-62696	7.8 HIGH
CVE-2026-62699	6.8 MEDIUM
CVE-2026-62703	5.5 MEDIUM
CVE-2026-62707	7.8 HIGH
CVE-2026-62713	7.8 HIGH
CVE-2026-62712	7.8 HIGH
CVE-2026-62718	6.5 MEDIUM
CVE-2026-62715	6.5 MEDIUM
CVE-2026-62716	6.5 MEDIUM
CVE-2026-62719	7.8 HIGH
CVE-2026-62723	7.0 HIGH
CVE-2026-62724	7.0 HIGH
CVE-2026-62748	7.0 HIGH
CVE-2026-62729	7.0 HIGH
CVE-2026-62738	5.5 MEDIUM
CVE-2026-62746	5.5 MEDIUM
CVE-2026-62740	5.5 MEDIUM
CVE-2026-62753	7.0 HIGH
CVE-2026-62735	7.8 HIGH

CVE-2026-62739	7.8 HIGH
CVE-2026-62742	6.5 MEDIUM
CVE-2026-62745	6.5 MEDIUM
CVE-2026-62747	7.8 HIGH
CVE-2026-62750	6.5 MEDIUM
CVE-2026-62754	7.8 HIGH
CVE-2026-62783	7.8 HIGH
CVE-2026-62755	7.8 HIGH
CVE-2026-62758	7.8 HIGH
CVE-2026-62773	7.0 HIGH
CVE-2026-62774	7.0 HIGH
CVE-2026-62785	8.8 HIGH
CVE-2026-62777	7.8 HIGH
CVE-2026-62792	8.1 HIGH
CVE-2026-62784	8.8 HIGH
CVE-2026-62787	7.5 HIGH
CVE-2026-62795	8.8 HIGH
CVE-2026-62796	5.5 MEDIUM
CVE-2026-62797	7.8 HIGH
CVE-2026-62812	7.8 HIGH
CVE-2026-62816	8.8 HIGH
CVE-2026-62817	8.8 HIGH
CVE-2026-62818	8.8 HIGH

CVE-2026-62819	8.1 HIGH
CVE-2026-62820	8.1 HIGH
CVE-2026-62876	7.8 HIGH
CVE-2026-62877	7.8 HIGH
CVE-2026-62878	9.8 CRITICAL
CVE-2026-62889	8.1 HIGH
CVE-2026-62890	7.8 HIGH
CVE-2026-62892	7.0 HIGH
CVE-2026-62893	9.8 CRITICAL
CVE-2026-62894	7.8 HIGH
CVE-2026-62908	7.0 HIGH
CVE-2026-65662	5.5 MEDIUM
CVE-2026-65671	7.8 HIGH
CVE-2026-65678	7.0 HIGH
CVE-2026-65784	5.5 MEDIUM
CVE-2026-65786	7.8 HIGH
CVE-2026-65789	8.1 HIGH
CVE-2026-65787	7.8 HIGH
CVE-2026-65814	7.8 HIGH
CVE-2026-66799	7.8 HIGH
CVE-2026-68819	5.9 MEDIUM
CVE-2026-68820	7.0 HIGH
CVE-2026-70307	7.0 HIGH

CVE-2026-70304	6.7 MEDIUM
CVE-2026-70330	6.7 MEDIUM
CVE-2026-61352	7.5 HIGH
CVE-2026-70344	7.8 HIGH
CVE-2026-70345	7.8 HIGH
CVE-2026-70346	7.8 HIGH
CVE-2026-70347	7.8 HIGH
CVE-2026-42976	7.8 HIGH
CVE-2026-6726	7.9 HIGH
CVE-2026-59122	7.0 HIGH
CVE-2026-59125	7.0 HIGH
CVE-2026-59131	5.6 MEDIUM
CVE-2026-61349	7.8 HIGH
CVE-2026-61363	7.5 HIGH
CVE-2026-61364	7.8 HIGH
CVE-2026-61365	7.8 HIGH
CVE-2026-61358	7.8 HIGH
CVE-2026-61360	5.5 MEDIUM
CVE-2026-61920	6.6 MEDIUM
CVE-2026-61926	7.8 HIGH
CVE-2026-61918	6.5 MEDIUM
CVE-2026-61921	6.5 MEDIUM
CVE-2026-62698	7.8 HIGH

CVE-2026-62700	7.8 HIGH
CVE-2026-62701	7.8 HIGH
CVE-2026-62709	5.5 MEDIUM
CVE-2026-62710	7.8 HIGH
CVE-2026-62711	7.8 HIGH
CVE-2026-62720	6.5 MEDIUM
CVE-2026-62714	6.5 MEDIUM
CVE-2026-62717	7.8 HIGH
CVE-2026-62721	7.8 HIGH
CVE-2026-62725	7.0 HIGH
CVE-2026-62726	7.0 HIGH
CVE-2026-62728	7.0 HIGH
CVE-2026-62733	7.8 HIGH
CVE-2026-62743	5.5 MEDIUM
CVE-2026-62730	5.5 MEDIUM
CVE-2026-62732	7.8 HIGH
CVE-2026-62734	7.0 HIGH
CVE-2026-62757	5.3 MEDIUM
CVE-2026-62741	7.8 HIGH
CVE-2026-62752	7.8 HIGH
CVE-2026-62769	6.7 MEDIUM
CVE-2026-62771	7.8 HIGH
CVE-2026-62761	7.8 HIGH

CVE-2026-62768	7.8 HIGH
CVE-2026-62770	7.8 HIGH
CVE-2026-62776	7.8 HIGH
CVE-2026-62778	8.1 HIGH
CVE-2026-62782	6.5 MEDIUM
CVE-2026-62781	8.1 HIGH
CVE-2026-62800	8.8 HIGH
CVE-2026-62786	5.5 MEDIUM
CVE-2026-62790	8.8 HIGH
CVE-2026-62793	5.5 MEDIUM
CVE-2026-62803	7.8 HIGH
CVE-2026-62807	7.8 HIGH
CVE-2026-62814	6.5 MEDIUM
CVE-2026-62823	8.8 HIGH
CVE-2026-62822	8.8 HIGH
CVE-2026-62880	7.8 HIGH
CVE-2026-62881	6.7 MEDIUM
CVE-2026-62883	6.7 MEDIUM
CVE-2026-62885	7.8 HIGH
CVE-2026-62887	5.5 MEDIUM
CVE-2026-65681	7.5 HIGH
CVE-2026-65679	8.1 HIGH
CVE-2026-65773	7.8 HIGH

CVE-2026-65774	7.8 HIGH
CVE-2026-65775	7.8 HIGH
CVE-2026-65790	7.8 HIGH
CVE-2026-65791	9.8 CRITICAL
CVE-2026-65795	6.7 MEDIUM
CVE-2026-65794	6.5 MEDIUM
CVE-2026-65797	6.7 MEDIUM
CVE-2026-65799	6.7 MEDIUM
CVE-2026-65798	6.7 MEDIUM
CVE-2026-65796	5.9 MEDIUM
CVE-2026-66802	8.1 HIGH
CVE-2026-71331	8.1 HIGH
CVE-2026-62695	7.8 HIGH
CVE-2026-62702	6.8 MEDIUM
CVE-2026-62815	9.8 CRITICAL
CVE-2026-65672	7.8 HIGH
CVE-2026-59126	7.0 HIGH
CVE-2026-61359	7.8 HIGH
CVE-2026-61355	7.8 HIGH
CVE-2026-62751	7.8 HIGH
CVE-2026-62811	7.8 HIGH
CVE-2026-62832	7.8 HIGH
CVE-2026-62888	7.8 HIGH

CVE-2026-65777	5.3 MEDIUM
CVE-2026-61361	7.0 HIGH
CVE-2026-61927	7.0 HIGH
CVE-2026-61933	5.5 MEDIUM
CVE-2026-61934	7.8 HIGH
CVE-2026-62722	7.8 HIGH
CVE-2026-62737	7.8 HIGH
CVE-2026-62766	7.0 HIGH
CVE-2026-62779	7.8 HIGH
CVE-2026-62798	5.5 MEDIUM
CVE-2026-65785	6.5 MEDIUM
CVE-2026-65788	7.0 HIGH
CVE-2026-61357	7.8 HIGH
CVE-2026-61929	7.0 HIGH
CVE-2026-61938	7.0 HIGH
CVE-2026-62708	6.4 MEDIUM
CVE-2026-62736	7.8 HIGH
CVE-2026-62749	7.0 HIGH
CVE-2026-62780	7.0 HIGH
CVE-2026-62788	7.0 HIGH
CVE-2026-65776	7.0 HIGH
CVE-2026-56179	8.3 HIGH
CVE-2026-62688	7.8 HIGH

CVE-2026-62705	7.0 HIGH
CVE-2026-66804	7.8 HIGH
CVE-2026-62693	7.0 HIGH
CVE-2026-65783	7.0 HIGH
CVE-2026-70348	5.5 MEDIUM
CVE-2026-65779	7.0 HIGH
CVE-2026-65780	7.0 HIGH
CVE-2026-65778	7.0 HIGH
CVE-2026-65782	7.0 HIGH
CVE-2026-65781	7.0 HIGH
CVE-2026-62772	7.8 HIGH
CVE-2026-62775	5.5 MEDIUM
CVE-2026-62799	7.8 HIGH
CVE-2026-62824	8.8 HIGH
CVE-2026-59124	9.8 CRITICAL
CVE-2026-59133	8.8 HIGH

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-187	Partial String Comparison
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-208	Observable Timing Discrepancy
CWE-250	Execution with Unnecessary Privileges
CWE-284	Improper Access Control
CWE-306	Missing Authentication for Critical Function
CWE-312	Cleartext Storage of Sensitive Information
CWE-326	Inadequate Encryption Strength
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
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-415	Double Free
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-427	Uncontrolled Search Path Element
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data

CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-908	Use of Uninitialized Resource
CWE-1220	Insufficient Granularity of Access Control
CWE-1390	Weak Authentication

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 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 11 Version 26H1 for ARM64-based Systems
Windows 11 version 26H1 for x64-based Systems
Windows App Client for Windows Desktop
Windows Remote Help
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)

Disclaimer