



# NCSC-2025-0310

## Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory

**PRIORITEIT: HOOG**

Gepubliceerd op: 24-10-2025

Revisie: 1.0.2

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Update Revisie 2

Het NCSC heeft van een vertrouwde partner vernomen dat op 24 oktober 2025 misbruik van CVE-2025-59287 is waargenomen. Tevens is er publieke proof-of-conceptcode beschikbaar voor de betreffende CVE, wat het risico op misbruik verhoogt. Het is goed gebruik om WSUS niet direct aan het internet te ontsluiten.

## 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
- Omzeilen van een beveiligingsmaatregel
- Manipulatie van gegevens
- Uitvoeren van willekeurige code (gebruikersrechten)
- Uitvoeren van willekeurige code (root/adminrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten
- Spoofing

De ernstigste kwetsbaarheden hebben de kenmerken CVE-2025-49708 en CVE-2025-59287 toegewezen gekregen. De kwetsbaarheid met kenmerk CVE-2025-49708 bevindt zich in de Graphics Component en stelt een kwaadwillende in staat om uit een Virtual Machine (VM) te breken en acties uit te voeren op de onderliggende Host. De kwetsbaarheid met kenmerk CVE-2025-59287 bevindt zich in de Windows Server Update Service (WSUS) en stelt een kwaadwillende in staat om op afstand willekeurige code uit te voeren op het kwetsbare systeem.

Van de kwetsbaarheid met kenmerk CVE-2025-59230 meldt Microsoft informatie te hebben dat deze actief is misbruikt op verouderde systemen. De kwetsbaarheid bevindt zich in de Remote Access Connection Manager stelt een lokale, geauthenticeerde kwaadwillende in staat om zich SYSTEM-rechten toe te kennen en zo mogelijk willekeurige code uit te voeren als SYSTEM

### Update:

Het NCSC heeft van een vertrouwde partner vernomen dat op 24 oktober 2025 misbruik van de kwetsbaarheid met kenmerk CVE-2025-59287 is waargenomen. Deze kwetsbaarheid bevindt zich in de WSUS-service en stelt een kwaadwillende in staat om willekeurige code uit te voeren op het kwetsbare systeem. Het is niet gebruikelijk

een WSUS service publiek via internet toegankelijk te hebben. Inmiddels is er publieke proof-of-conceptcode beschikbaar voor de betreffende kwetsbaarheid, wat het risico op misbruik verhoogt.

**De in deze Patch-Tuesday update uitgebrachte oplossing voor deze kwetsbaarheid blijkt niet afdoende te zijn. Microsoft heeft hiervoor een out-of-band patch uitgebracht die zo spoedig mogelijk aanvullend op de Patch-Tuesday update dient te worden ingezet.**

Windows Confidential Virtual Machines (CVM):

CVE-ID	CVSS	Impact
CVE-2025-48813	6.30	Voordoens als andere gebruiker

Windows Resilient File System (ReFS):

CVE-ID	CVSS	Impact
CVE-2025-55687	7.40	Verkrijgen van verhoogde rechten

Windows DirectX:

CVE-ID	CVSS	Impact
CVE-2025-55678	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55698	7.70	Denial-of-Service

Windows DWM:

CVE-ID	CVSS	Impact
CVE-2025-55681	7.00	Verkrijgen van verhoogde rechten
CVE-2025-58722	7.80	Verkrijgen van verhoogde rechten

Xbox:

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

CVE-2025-53768	7.80	Verkrijgen van verhoogde rechten
----------------	------	----------------------------------

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-59186	5.50	Toegang tot gevoelige gegevens
CVE-2025-59207	7.80	Verkrijgen van verhoogde rechten
CVE-2025-50152	7.80	Verkrijgen van verhoogde rechten
CVE-2025-55334	6.20	Omzeilen van beveiligingsmaatregel
CVE-2025-55679	5.10	Toegang tot gevoelige gegevens
CVE-2025-55683	5.50	Toegang tot gevoelige gegevens
CVE-2025-55693	7.40	Verkrijgen van verhoogde rechten
CVE-2025-55699	5.50	Toegang tot gevoelige gegevens
CVE-2025-59187	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59194	7.00	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-55700	6.50	Toegang tot gevoelige gegevens
CVE-2025-58717	6.50	Toegang tot gevoelige gegevens

Inbox COM Objects:

CVE-ID	CVSS	Impact
CVE-2025-58732	7.00	Uitvoeren van willekeurige code
CVE-2025-58735	7.00	Uitvoeren van willekeurige code
CVE-2025-59282	7.00	Uitvoeren van willekeurige code
CVE-2025-58730	7.00	Uitvoeren van willekeurige code
CVE-2025-58731	7.00	Uitvoeren van willekeurige code
CVE-2025-58733	7.00	Uitvoeren van willekeurige code
CVE-2025-58734	7.00	Uitvoeren van willekeurige code
CVE-2025-58736	7.00	Uitvoeren van willekeurige code
CVE-2025-58738	7.00	Uitvoeren van willekeurige code

Agere Windows Modem Driver:

CVE-ID	CVSS	Impact
CVE-2025-24990	7.80	Verkrijgen van verhoogde rechten
CVE-2025-24052	7.80	Verkrijgen van verhoogde rechten

Active Directory Federation Services:

CVE-ID	CVSS	Impact
CVE-2025-59258	6.20	Toegang tot gevoelige gegevens

Windows Push Notification Core:

CVE-ID	CVSS	Impact
CVE-2025-59211	5.50	Toegang tot gevoelige gegevens
CVE-2025-59209	5.50	Toegang tot gevoelige gegevens

Windows Authentication Methods:

CVE-ID	CVSS	Impact
CVE-2025-59277	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59275	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59278	7.80	Verkrijgen van verhoogde rechten

Windows File Explorer:

CVE-ID	CVSS	Impact
CVE-2025-58739	6.50	Voordoen als andere gebruiker
CVE-2025-59214	6.50	Voordoen als andere gebruiker

Data Sharing Service Client:

CVE-ID	CVSS	Impact
CVE-2025-59200	7.70	Voordoen als andere gebruiker

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-55328	7.80	Verkrijgen van verhoogde rechten

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-55335	7.40	Verkrijgen van verhoogde rechten

Windows ETL Channel:

CVE-ID	CVSS	Impact
CVE-2025-59197	5.50	Toegang tot gevoelige gegevens

Microsoft Failover Cluster Virtual Driver:

CVE-ID	CVSS	Impact
CVE-2025-59260	5.50	Toegang tot gevoelige gegevens

Windows Server Update Service:

CVE-ID	CVSS	Impact
CVE-2025-59287	9.80	Uitvoeren van willekeurige code

Microsoft Windows Speech:

CVE-ID	CVSS	Impact
CVE-2025-58715	8.80	Verkrijgen van verhoogde rechten
CVE-2025-58716	8.80	Verkrijgen van verhoogde rechten

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2025-59284	3.30	Voordoen als andere gebruiker

Windows COM:

CVE-ID	CVSS	Impact
CVE-2025-58725	7.00	Verkrijgen van verhoogde rechten

Network Connection Status Indicator (NCSI):

CVE-ID	CVSS	Impact
CVE-2025-59201	7.80	Verkrijgen van verhoogde rechten

TCG TPM2.0:

CVE-ID	CVSS	Impact
CVE-2025-2884	5.30	Toegang tot gevoelige gegevens

Windows MapUrlToZone:

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

CVE-2025-59208	7.10	Toegang tot gevoelige gegevens
----------------	------	--------------------------------

Internet Explorer:

CVE-ID	CVSS	Impact
CVE-2025-59295	8.80	Uitvoeren van willekeurige code

Windows Core Shell:

CVE-ID	CVSS	Impact
CVE-2025-59185	6.50	Voordoen als andere gebruiker
CVE-2025-59244	6.50	Voordoen als andere gebruiker

Windows SMB Server:

CVE-ID	CVSS	Impact
CVE-2025-58726	7.50	Verkrijgen van verhoogde rechten

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact
CVE-2025-59230	7.80	Verkrijgen van verhoogde rechten

Windows PrintWorkflowUserSvc:

CVE-ID	CVSS	Impact
CVE-2025-55685	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55686	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55689	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55331	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55684	7.00	Verkrijgen van verhoogde rechten

CVE-2025-55688	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55690	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55691	7.00	Verkrijgen van verhoogde rechten

Windows Taskbar Live:

CVE-ID	CVSS	Impact
CVE-2025-59294	2.10	Toegang tot gevoelige gegevens

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2025-55333	6.10	Omzeilen van beveiligingsmaatregel
CVE-2025-55338	6.10	Omzeilen van beveiligingsmaatregel
CVE-2025-55330	6.10	Omzeilen van beveiligingsmaatregel
CVE-2025-55332	6.10	Omzeilen van beveiligingsmaatregel
CVE-2025-55337	6.10	Omzeilen van beveiligingsmaatregel
CVE-2025-55682	6.10	Omzeilen van beveiligingsmaatregel

NtQueryInformation Token function (ntifs.h):

CVE-ID	CVSS	Impact
CVE-2025-55696	7.80	Verkrijgen van verhoogde rechten

Windows USB Video Driver:

CVE-ID	CVSS	Impact
CVE-2025-55676	5.50	Toegang tot gevoelige gegevens

Windows Ancillary Function Driver for WinSock:

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

CVE-ID	CVSS	Impact
CVE-2025-59242	7.80	Verkrijgen van verhoogde rechten
CVE-2025-58714	7.80	Verkrijgen van verhoogde rechten

Azure Local:

CVE-ID	CVSS	Impact
CVE-2025-55697	7.80	Verkrijgen van verhoogde rechten

Windows Local Session Manager (LSM):

CVE-ID	CVSS	Impact
CVE-2025-59257	6.50	Denial-of-Service
CVE-2025-59259	6.50	Denial-of-Service
CVE-2025-58729	6.50	Denial-of-Service

Windows Resilient File System (ReFS) Deduplication Service:

CVE-ID	CVSS	Impact
CVE-2025-59206	7.40	Verkrijgen van verhoogde rechten
CVE-2025-59210	7.40	Verkrijgen van verhoogde rechten

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
CVE-2025-53717	7.00	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2025-55336	5.50	Toegang tot gevoelige gegevens

CVE-2025-55680	8.40	Verkrijgen van verhoogde rechten
----------------	------	----------------------------------

Windows WLAN Auto Config Service:

CVE-ID	CVSS	Impact
CVE-2025-55695	5.50	Toegang tot gevoelige gegevens

Software Protection Platform (SPP):

CVE-ID	CVSS	Impact
CVE-2025-59199	8.40	Verkrijgen van verhoogde rechten

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2025-58720	7.80	Toegang tot gevoelige gegevens

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2025-58718	8.80	Uitvoeren van willekeurige code

Windows StateRepository API:

CVE-ID	CVSS	Impact
CVE-2025-59203	5.50	Toegang tot gevoelige gegevens

Microsoft Windows Search Component:

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

CVE-ID	CVSS	Impact
CVE-2025-59190	5.50	Denial-of-Service
CVE-2025-59198	5.00	Denial-of-Service
CVE-2025-59253	5.50	Denial-of-Service

Windows Failover Cluster:

CVE-ID	CVSS	Impact
CVE-2025-47979	5.50	Toegang tot gevoelige gegevens
CVE-2025-59188	5.50	Toegang tot gevoelige gegevens

Windows SMB Client:

CVE-ID	CVSS	Impact
CVE-2025-59280	3.10	Manipulatie van gegevens

Windows Secure Boot:

CVE-ID	CVSS	Impact
CVE-2025-47827	4.60	Omzeilen van beveiligingsmaatregel

Microsoft PowerShell:

CVE-ID	CVSS	Impact
CVE-2025-25004	7.30	Verkrijgen van verhoogde rechten

Microsoft Windows:

CVE-ID	CVSS	Impact
CVE-2025-55701	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows Codecs Library:

CVE-ID	CVSS	Impact
CVE-2025-54957	7.00	Uitvoeren van willekeurige code

Windows Error Reporting:

CVE-ID	CVSS	Impact
CVE-2025-55692	7.80	Verkrijgen van verhoogde rechten
CVE-2025-55694	7.80	Verkrijgen van verhoogde rechten

Windows SSDP Service:

CVE-ID	CVSS	Impact
CVE-2025-59196	7.00	Verkrijgen van verhoogde rechten

Storport.sys Driver:

CVE-ID	CVSS	Impact
CVE-2025-59192	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop Protocol:

CVE-ID	CVSS	Impact
CVE-2025-55340	7.00	Omzeilen van beveiligingsmaatregel

Windows Connected Devices Platform Service:

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

CVE-2025-58727	7.00	Verkrijgen van verhoogde rechten
----------------	------	----------------------------------

Windows NDIS:

CVE-ID	CVSS	Impact
CVE-2025-55339	7.80	Verkrijgen van verhoogde rechten

Windows Health and Optimized Experiences Service:

CVE-ID	CVSS	Impact
CVE-2025-59241	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop Services:

CVE-ID	CVSS	Impact
CVE-2025-59202	7.00	Verkrijgen van verhoogde rechten

Windows High Availability Services:

CVE-ID	CVSS	Impact
CVE-2025-59184	5.50	Toegang tot gevoelige gegevens

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2025-48004	7.40	Verkrijgen van verhoogde rechten
CVE-2025-59189	7.40	Verkrijgen van verhoogde rechten

Windows DWM Core Library:

--	--	--

CVE-ID	CVSS	Impact
CVE-2025-59254	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59255	7.80	Verkrijgen van verhoogde rechten

Windows Digital Media:

CVE-ID	CVSS	Impact
CVE-2025-53150	7.80	Verkrijgen van verhoogde rechten
CVE-2025-50175	7.80	Verkrijgen van verhoogde rechten

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2025-53139	7.70	Omzeilen van beveiligingsmaatregel

Connected Devices Platform Service (Cdpsvc):

CVE-ID	CVSS	Impact
CVE-2025-58719	4.70	Verkrijgen van verhoogde rechten
CVE-2025-55326	7.50	Uitvoeren van willekeurige code
CVE-2025-59191	7.80	Verkrijgen van verhoogde rechten

Windows Device Association Broker service:

CVE-ID	CVSS	Impact
CVE-2025-50174	7.00	Verkrijgen van verhoogde rechten
CVE-2025-55677	7.80	Verkrijgen van verhoogde rechten

Windows Bluetooth Service:

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

CVE-2025-58728	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59290	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59289	7.00	Verkrijgen van verhoogde rechten

Windows Storage Management Provider:

CVE-ID	CVSS	Impact
CVE-2025-55325	5.50	Toegang tot gevoelige gegevens

Windows Management Services:

CVE-ID	CVSS	Impact
CVE-2025-59204	5.50	Toegang tot gevoelige gegevens
CVE-2025-59193	7.00	Verkrijgen van verhoogde rechten

Windows Remote Desktop:

CVE-ID	CVSS	Impact
CVE-2025-58737	7.00	Uitvoeren van willekeurige code

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2025-59195	7.00	Denial-of-Service
CVE-2025-49708	9.90	Uitvoeren van willekeurige code
CVE-2016-9535	4.00	Uitvoeren van willekeurige code
CVE-2025-59205	7.00	Verkrijgen van verhoogde rechten
CVE-2025-59261	7.00	Verkrijgen van verhoogde rechten

**Update:** Het NCSC heeft van een vertrouwde partner vernomen dat op 24 oktober 2025 misbruik van CVE-2025-59287 is waargenomen. Tevens is er publieke proof-of-conceptcode beschikbaar voor de betreffende CVE, wat het risico op misbruik verhoogt. Het is goed gebruik om WSUS niet direct aan het internet te ontsluiten.

## 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>

Voor aanvullende informatie en eventuele workarounds met betrekking tot de kwetsbaarheid met kenmerk CVE-2025-59287 heeft microsoft de informatie bij deze kwetsbaarheid geactualiseerd. Zie de detailpagina op:

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287>

## Referenties

➤ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-59258</a>	6.2 MEDIUM
➤ <a href="#">CVE-2025-47979</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-55683</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-55697</a>	7.8 HIGH
➤ <a href="#">CVE-2025-58737</a>	7.0 HIGH
➤ <a href="#">CVE-2025-59184</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-59188</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-59260</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-59287</a>	9.8 CRITICAL
➤ <a href="#">CVE-2025-48004</a>	7.4 HIGH
➤ <a href="#">CVE-2025-50174</a>	7.0 HIGH

> CVE-2025-24990	7.8 HIGH
> CVE-2025-24052	7.8 HIGH
> CVE-2025-55325	5.5 MEDIUM
> CVE-2025-55333	6.1 MEDIUM
> CVE-2025-55335	7.4 HIGH
> CVE-2025-55336	5.5 MEDIUM
> CVE-2025-55338	6.1 MEDIUM
> CVE-2025-55339	7.8 HIGH
> CVE-2025-55340	7.0 HIGH
> CVE-2025-55676	5.5 MEDIUM
> CVE-2025-55677	7.8 HIGH
> CVE-2025-55681	7.0 HIGH
> CVE-2025-55685	7.0 HIGH
> CVE-2025-55686	7.0 HIGH
> CVE-2025-55687	7.4 HIGH
> CVE-2025-55689	7.0 HIGH
> CVE-2025-55700	6.5 MEDIUM
> CVE-2025-55701	7.8 HIGH
> CVE-2025-58715	8.8 HIGH
> CVE-2025-58716	8.8 HIGH
> CVE-2025-58717	6.5 MEDIUM
> CVE-2025-58719	4.7 MEDIUM
> CVE-2025-58722	7.8 HIGH

> CVE-2025-58728	7.8 HIGH
> CVE-2025-58732	7.0 HIGH
> CVE-2025-58735	7.0 HIGH
> CVE-2025-59185	6.5 MEDIUM
> CVE-2025-59195	7.0 HIGH
> CVE-2025-59196	7.0 HIGH
> CVE-2025-59199	7.8 HIGH
> CVE-2025-59200	7.7 HIGH
> CVE-2025-59201	7.8 HIGH
> CVE-2025-59202	7.0 HIGH
> CVE-2025-59204	5.5 MEDIUM
> CVE-2025-59206	7.4 HIGH
> CVE-2025-59207	7.8 HIGH
> CVE-2025-59211	5.5 MEDIUM
> CVE-2025-59242	7.8 HIGH
> CVE-2025-49708	9.9 CRITICAL
> CVE-2025-59254	7.8 HIGH
> CVE-2025-59255	7.8 HIGH
> CVE-2025-54957	7.0 HIGH
> CVE-2025-59257	6.5 MEDIUM
> CVE-2025-59259	6.5 MEDIUM
> CVE-2025-59282	7.0 HIGH
> CVE-2025-59284	3.3 LOW

> CVE-2025-59294	2.1 LOW
> CVE-2025-59295	8.8 HIGH
> CVE-2016-9535	9.8 CRITICAL
> CVE-2025-48813	6.3 MEDIUM
> CVE-2025-25004	7.3 HIGH
> CVE-2025-53717	7.0 HIGH
> CVE-2025-50152	7.8 HIGH
> CVE-2025-53150	7.8 HIGH
> CVE-2025-50175	7.8 HIGH
> CVE-2025-53139	7.7 HIGH
> CVE-2025-53768	7.8 HIGH
> CVE-2025-55328	7.8 HIGH
> CVE-2025-55330	6.1 MEDIUM
> CVE-2025-55331	7.0 HIGH
> CVE-2025-55332	6.1 MEDIUM
> CVE-2025-55334	6.2 MEDIUM
> CVE-2025-55337	6.1 MEDIUM
> CVE-2025-55678	7.0 HIGH
> CVE-2025-55679	5.1 MEDIUM
> CVE-2025-55680	7.8 HIGH
> CVE-2025-55682	6.1 MEDIUM
> CVE-2025-55684	7.0 HIGH
> CVE-2025-55688	7.0 HIGH

> CVE-2025-55690	7.0 HIGH
> CVE-2025-55691	7.0 HIGH
> CVE-2025-55692	7.8 HIGH
> CVE-2025-55693	7.4 HIGH
> CVE-2025-55694	7.8 HIGH
> CVE-2025-55695	5.5 MEDIUM
> CVE-2025-55696	7.8 HIGH
> CVE-2025-55698	7.7 HIGH
> CVE-2025-55699	5.5 MEDIUM
> CVE-2025-58714	7.8 HIGH
> CVE-2025-58718	8.8 HIGH
> CVE-2025-58720	7.8 HIGH
> CVE-2025-58725	7.0 HIGH
> CVE-2025-58726	7.5 HIGH
> CVE-2025-58727	7.0 HIGH
> CVE-2025-58729	6.5 MEDIUM
> CVE-2025-58730	7.0 HIGH
> CVE-2025-58731	7.0 HIGH
> CVE-2025-58733	7.0 HIGH
> CVE-2025-58734	7.0 HIGH
> CVE-2025-58736	7.0 HIGH
> CVE-2025-58738	7.0 HIGH
> CVE-2025-58739	6.5 MEDIUM

> CVE-2025-59187	7.8 HIGH
> CVE-2025-59189	7.4 HIGH
> CVE-2025-59190	5.5 MEDIUM
> CVE-2025-59191	7.8 HIGH
> CVE-2025-59192	7.8 HIGH
> CVE-2025-59193	7.0 HIGH
> CVE-2025-59194	7.0 HIGH
> CVE-2025-59197	5.5 MEDIUM
> CVE-2025-59198	5.0 MEDIUM
> CVE-2025-59203	5.5 MEDIUM
> CVE-2025-59205	7.0 HIGH
> CVE-2025-59208	7.1 HIGH
> CVE-2025-59209	5.5 MEDIUM
> CVE-2025-59210	7.4 HIGH
> CVE-2025-59214	6.5 MEDIUM
> CVE-2025-59241	7.8 HIGH
> CVE-2025-2884	6.6 MEDIUM
> CVE-2025-59244	6.5 MEDIUM
> CVE-2025-59230	7.8 HIGH
> CVE-2025-59253	5.5 MEDIUM
> CVE-2025-59261	7.0 HIGH
> CVE-2025-47827	2.0 LOW
> CVE-2025-59277	7.8 HIGH

> CVE-2025-59280	3.1 LOW
> CVE-2025-59290	7.8 HIGH
> CVE-2025-55326	7.5 HIGH
> CVE-2025-59275	7.8 HIGH
> CVE-2025-59278	7.8 HIGH
> CVE-2025-59289	7.0 HIGH
> CVE-2025-59186	5.5 MEDIUM

## 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-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> 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-209	Generation of Error Message Containing Sensitive Information
> CWE-284	Improper Access Control
> CWE-287	Improper Authentication

➤ CWE-312	Cleartext Storage of Sensitive Information
➤ CWE-319	Cleartext Transmission of Sensitive Information
➤ CWE-324	Use of a Key Past its Expiration Date
➤ 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-415	Double Free
➤ CWE-416	Use After Free
➤ CWE-476	NULL Pointer Dereference
➤ CWE-502	Deserialization of Untrusted Data
➤ CWE-532	Insertion of Sensitive Information into Log File
➤ CWE-807	Reliance on Untrusted Inputs in a Security Decision
➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-841	Improper Enforcement of Behavioral Workflow
➤ CWE-908	Use of Uninitialized Resource
➤ CWE-1023	Incomplete Comparison with Missing Factors
➤ CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
➤ CWE-1287	Improper Validation of Specified Type of Input

## Getroffen producten

<b>Microsoft</b>
Windows 10 1809
Windows 10 21h2

Windows 10 22h2
Windows 10 Version 1507
Windows 10 Version 1607
Windows 10 Version 1809
Windows 10 Version 21H2
Windows 10 Version 22H2
Windows 11 22H2
Windows 11 23H2
Windows 11 Version 23H2
Windows 11 Version 24H2
Windows 11 Version 25H2
Windows 11 version 22H2
Windows 11 version 22H3
Windows Server 2008 R2 Service Pack 1
Windows Server 2008 R2 Service Pack 1 (Server Core installation)
Windows Server 2008 Service Pack 2

Windows Server 2008 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)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022, 23H2 Edition (Server Core installation)
Windows Server 2025
Windows Server 2025 (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.