



NCSC-2025-0383

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-12-2025

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
- Uitvoeren van willekeurige code (root/adminrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten

Windows DirectX:

CVE-ID	CVSS	Impact
CVE-2025-62573	7.00	Verkrijgen van verhoogde rechten
CVE-2025-62463	6.50	Denial-of-Service
CVE-2025-62465	6.50	Denial-of-Service

Windows Projected File System Filter Driver:

CVE-ID	CVSS	Impact
CVE-2025-62461	7.80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-62473	6.50	Toegang tot gevoelige gegevens
CVE-2025-62549	8.80	Uitvoeren van willekeurige code
CVE-2025-64678	8.80	Uitvoeren van willekeurige code

Windows Defender Firewall Service:

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

CVE-ID	CVSS	Impact
CVE-2025-62468	4.40	Toegang tot gevoelige gegevens

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact
CVE-2025-62472	7.80	Verkrijgen van verhoogde rechten
CVE-2025-62474	7.80	Verkrijgen van verhoogde rechten

Windows Shell:

CVE-ID	CVSS	Impact
CVE-2025-64658	7.50	Verkrijgen van verhoogde rechten
CVE-2025-62565	7.30	Verkrijgen van verhoogde rechten
CVE-2025-64661	7.80	Verkrijgen van verhoogde rechten

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2025-64679	7.80	Verkrijgen van verhoogde rechten
CVE-2025-64680	7.80	Verkrijgen van verhoogde rechten

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2025-62469	7.00	Verkrijgen van verhoogde rechten
CVE-2025-62569	7.00	Verkrijgen van verhoogde rechten

Windows Win32K - GRFX:

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

CVE-2025-62458	7.80	Verkrijgen van verhoogde rechten

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2025-62571	7.80	Verkrijgen van verhoogde rechten

Windows Camera Frame Server Monitor:

CVE-ID	CVSS	Impact
CVE-2025-62570	7.10	Toegang tot gevoelige gegevens

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2025-62454	7.80	Verkrijgen van verhoogde rechten
CVE-2025-62457	7.80	Verkrijgen van verhoogde rechten
CVE-2025-62221	7.80	Verkrijgen van verhoogde rechten

Storvsp.sys Driver:

CVE-ID	CVSS	Impact
CVE-2025-64673	7.80	Verkrijgen van verhoogde rechten

Windows Projected File System:

CVE-ID	CVSS	Impact
CVE-2025-62462	7.80	Verkrijgen van verhoogde rechten
CVE-2025-62464	7.80	Verkrijgen van verhoogde rechten
CVE-2025-55233	7.80	Verkrijgen van verhoogde rechten

CVE-2025-62467	7.80	Verkrijgen van verhoogde rechten
----------------	------	----------------------------------

Windows Client-Side Caching (CSC) Service:

CVE-ID	CVSS	Impact
CVE-2025-62466	7.80	Verkrijgen van verhoogde rechten

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2025-62455	7.80	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2025-62470	7.80	Verkrijgen van verhoogde rechten

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-62567	5.30	Denial-of-Service

Windows Storage VSP Driver:

CVE-ID	CVSS	Impact
CVE-2025-59516	7.80	Verkrijgen van verhoogde rechten
CVE-2025-59517	7.80	Verkrijgen van verhoogde rechten

Windows Resilient File System (ReFS):

--	--	--

CVE-ID	CVSS	Impact
CVE-2025-62456	8.80	Uitvoeren van willekeurige code

Application Information Services:

CVE-ID	CVSS	Impact
CVE-2025-62572	7.80	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2025-64670	6.50	Toegang tot gevoelige gegevens

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-2025-62454	7.8 HIGH
> CVE-2025-62456	8.8 HIGH
> CVE-2025-62457	7.8 HIGH
> CVE-2025-62466	7.8 HIGH
> CVE-2025-62469	7.0 HIGH

> CVE-2025-62470	7.8 HIGH
> CVE-2025-62472	7.8 HIGH
> CVE-2025-62473	6.5 MEDIUM
> CVE-2025-62549	8.8 HIGH
> CVE-2025-62571	7.8 HIGH
> CVE-2025-62572	7.8 HIGH
> CVE-2025-62573	7.0 HIGH
> CVE-2025-64658	7.5 HIGH
> CVE-2025-64670	6.5 MEDIUM
> CVE-2025-64673	7.8 HIGH
> CVE-2025-59516	7.8 HIGH
> CVE-2025-59517	7.8 HIGH
> CVE-2025-62461	7.8 HIGH
> CVE-2025-62462	7.8 HIGH
> CVE-2025-62463	6.5 MEDIUM
> CVE-2025-62464	7.8 HIGH
> CVE-2025-62465	6.5 MEDIUM
> CVE-2025-55233	7.8 HIGH
> CVE-2025-62467	7.8 HIGH
> CVE-2025-62468	4.4 MEDIUM
> CVE-2025-62474	7.8 HIGH
> CVE-2025-62567	5.3 MEDIUM
> CVE-2025-62569	7.0 HIGH

> CVE-2025-62570	7.1 HIGH
> CVE-2025-62565	7.3 HIGH
> CVE-2025-64661	7.8 HIGH
> CVE-2025-64678	8.8 HIGH
> CVE-2025-64679	7.8 HIGH
> CVE-2025-64680	7.8 HIGH
> CVE-2025-62221	7.8 HIGH
> CVE-2025-62458	7.8 HIGH
> CVE-2025-62455	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-73	External Control of File Name or Path
> 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-284	Improper Access Control
> CWE-306	Missing Authentication for Critical Function
> CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CWE-415	Double Free

➤ CWE-416	Use After Free
➤ CWE-476	NULL Pointer Dereference
➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-908	Use of Uninitialized Resource

Getroffen producten

Microsoft
Windows 10 1809
Windows 10 21h2
Windows 10 22h2
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 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 11 23H2
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 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 for ARM64-based Systems
Windows 11 Version 25H2 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems 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 (Server Core installation)
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.