Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0159

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 (DoS)
- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (root/adminrechten)
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot systeemgegevens
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten

```
Windows Trusted Runtime Interface Driver:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29829 | 5.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows File Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29839 | 4.00 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Remote Desktop:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29966 | 8.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Active Directory Certificate Services (AD CS):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

| CVE-2025-29968 | 6.50 | Denial-of-Service |

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2025-32709	7.80	Verkrijgen van verhoogde rechten

Windows Drivers:

CVE-ID	CVSS	Impact
CVE-2025-29838	7.40	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-29974	5.70	Toegang tot gevoelige gegevens
CVE-2025-24063	7.80	Verkrijgen van verhoogde rechten

Windows DWM:

CVE-ID	CVSS	Impact
CVE-2025-30400	7.80	Verkrijgen van verhoogde rechten

Microsoft Brokering File System:

CVE-ID	CVSS	Impact
CVE-2025-29970	7.80	Verkrijgen van verhoogde rechten

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2025-29837	5.50	Toegang tot gevoelige gegevens

Microsoft Scripting Engine:

CVE-ID	CVSS	Impact
CVE-2025-30397	7.50	Uitvoeren van willekeurige code

Windows Hardware Lab Kit:

CVE-ID	CVSS	Impact
CVE-2025-27488	6.70	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-29959	6.50	Toegang tot gevoelige gegevens
CVE-2025-29960	6.50	Toegang tot gevoelige gegevens
CVE-2025-29830	6.50	Toegang tot gevoelige gegevens
CVE-2025-29832	6.50	Toegang tot gevoelige gegevens
CVE-2025-29835	6.50	Toegang tot gevoelige gegevens
CVE-2025-29836	6.50	Toegang tot gevoelige gegevens
CVE-2025-29958	6.50	Toegang tot gevoelige gegevens
CVE-2025-29961	6.50	Toegang tot gevoelige gegevens

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-30388	7.80	Uitvoeren van willekeurige code

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2025-29955	6.20	Denial-of-Service

Web Threat Defense (WTD.sys):

CVE-ID	CVSS	Impact
CVE-2025-29971	7.50	Denial-of-Service

Windows NTFS:

CVE-ID	CVSS	Impact
CVE-2025-32707	7.80	Verkrijgen van verhoogde rechten

Remote Desktop Gateway Service:

CVE-ID	CVSS	Impact
CVE-2025-29967	8.80	Uitvoeren van willekeurige code
CVE-2025-30394	5.90	Denial-of-Service
CVE-2025-26677	7.50	Denial-of-Service
CVE-2025-29831	7.50	Uitvoeren van willekeurige code

Universal Print Management Service:

CVE-ID	CVSS	Impact
CVE-2025-29841	7.00	Verkrijgen van verhoogde rechten

Windows Media:

CVE-ID	CVSS	Impact

CVE-2025-29964	8.80	Uitvoeren van willekeurige code
CVE-2025-29840	8.80	Uitvoeren van willekeurige code
CVE-2025-29962	8.80	Uitvoeren van willekeurige code
CVE-2025-29963	8.80	Uitvoeren van willekeurige code

Windows Virtual Machine Bus:

CVE-ID	CVSS	Impact
CVE-2025-29833	7.10	Uitvoeren van willekeurige code

Windows SMB:

CVE-ID	CVSS	Impact
CVE-2025-29956	5.40	Toegang tot gevoelige gegevens

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2025-32701	7.80	Verkrijgen van verhoogde rechten
CVE-2025-32706	7.80	Verkrijgen van verhoogde rechten
CVE-2025-30385	7.80	Verkrijgen van verhoogde rechten

Windows Secure Kernel Mode:

CVE-ID	CVSS	Impact
CVE-2025-27468	7.00	Verkrijgen van verhoogde rechten

Windows Fundamentals:

CVE-ID	CVSS	Impact

```
| CVE-2025-29969 | 7.50 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Windows LDAP - Lightweight Directory Access Protocol:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29954 | 5.90 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows Deployment Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29957 | 6.20 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

UrlMon:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29842 | 7.50 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|
```

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-2025-29959	
CVE-2025-29960	
CVE-2025-29964	

CVE-2025-29966	
CVE-2025-29967	8.8 HIGH
CVE-2025-29969	7.5 HIGH
CVE-2025-27468	
CVE-2025-30400	
CVE-2025-32701	
CVE-2025-32706	7.8 HIGH
CVE-2025-32709	
CVE-2025-29829	
CVE-2025-29830	6.5 MEDIUM
CVE-2025-29832	6.5 MEDIUM
CVE-2025-29833	
CVE-2025-29835	6.5 MEDIUM
CVE-2025-29836	
CVE-2025-29837	
CVE-2025-29839	
CVE-2025-29840	
CVE-2025-29842	
CVE-2025-29954	5.9 MEDIUM
CVE-2025-29956	
CVE-2025-29957	6.2 MEDIUM
CVE-2025-29958	6.5 MEDIUM
CVE-2025-29961	

CVE-2025-29962	
CVE-2025-29963	
CVE-2025-29974	5.7 MEDIUM
CVE-2025-30385	
CVE-2025-30388	7.8 HIGH
CVE-2025-30397	7.5 HIGH
CVE-2025-32707	
CVE-2025-24063	
CVE-2025-29968	6.5 MEDIUM
CVE-2025-30394	
CVE-2025-26677	
CVE-2025-29831	
CVE-2025-29841	
CVE-2025-29971	7.5 HIGH
CVE-2025-29970	
CVE-2025-29838	
CVE-2025-29955	6.2 MEDIUM
CVE-2025-27488	

CWE's

CWE	Beschrijving
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-59	Improper Link Resolution Before File Access ('Link Following')

CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-126	Buffer Over-read
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-908	Use of Uninitialized Resource
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-798	Use of Hard-coded Credentials
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-400	Uncontrolled Resource Consumption
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-269	Improper Privilege Management
CWE-20	Improper Input Validation

Getroffen producten

Microsoft
Windows 10 Version 22H2 for x64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems

Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows Server 2022 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2016 (Server Core installation)
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows HLK for Windows Server 2025
Windows 11 Version 24H2 for x64-based Systems
Windows 11 Version 24H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 10 Version 22H2 for 32-bit Systems

Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows HLK for Windows Server 2019
Windows 10 21h2
Windows Server 2016
Windows Server 2025
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012
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 x64-based Systems Service Pack 2 (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 2022, 23H2 Edition (Server Core installation)

Windows Server 2025 (Server Core installation)
Microsoft Office LTSC for Mac 2024
Microsoft Office for Universal
Microsoft Office for Android
Microsoft Office LTSC for Mac 2021
IBM
Microsoft Windows Server 2022
Microsoft Windows Server 2012 R2 (Server Core installation)

Disclaimer