Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0188

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-06-2025

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
- Uitvoeren van willekeurige code (Gebruikersrechten)
- Uitvoeren van willekeurige code (Root/Adminrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten
- Spoofing

```
Windows Recovery Driver:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-32721 | 7.30 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Security App:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-47956 | 5.50 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|

App Control for Business (WDAC):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-33069 | 5.10 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|

Windows Remote Desktop Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

| CVE-2025-32710 | 8.10 | Uitvoeren van willekeurige code |

Windows Storage Management Provider:

CVE-ID	CVSS	Impact
CVE-2025-32719	5.50	Toegang tot gevoelige gegevens
CVE-2025-32720	5.50	Toegang tot gevoelige gegevens
CVE-2025-33058	5.50	Toegang tot gevoelige gegevens
CVE-2025-33059	5.50	Toegang tot gevoelige gegevens
CVE-2025-33060	5.50	Toegang tot gevoelige gegevens
CVE-2025-33061	5.50	Toegang tot gevoelige gegevens
CVE-2025-33062	5.50	Toegang tot gevoelige gegevens
CVE-2025-33063	5.50	Toegang tot gevoelige gegevens
CVE-2025-33065	5.50	Toegang tot gevoelige gegevens
CVE-2025-24068	5.50	Toegang tot gevoelige gegevens
CVE-2025-24069	5.50	Toegang tot gevoelige gegevens
CVE-2025-24065	5.50	Toegang tot gevoelige gegevens
CVE-2025-33055	5.50	Toegang tot gevoelige gegevens

Windows Local Security Authority Subsystem Service (LSASS):

CVE-ID	CVSS	Impact
CVE-2025-32724	7.50	Denial-of-Service

Windows KDC Proxy Service (KPSSVC):

CVE-ID	CVSS	Impact
CVE-2025-33071	8.10	Uitvoeren van willekeurige code

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact

CVE-2025-47955	7.80	Verkrijgen van verhoogde rechten

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2025-32715	6.50	Toegang tot gevoelige gegevens

Windows Storage Port Driver:

CVE-ID	CVSS	Impact
CVE-2025-32722	5.50	Toegang tot gevoelige gegevens

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2025-32714	7.80	Verkrijgen van verhoogde rechten
CVE-2025-33075	7.80	Verkrijgen van verhoogde rechten

Windows Hello:

CVE-ID	CVSS	Impact
CVE-2025-47969	4.40	Toegang tot gevoelige gegevens

WebDAV:

CVE-ID	CVSS	Impact
CVE-2025-33053	8.80	Uitvoeren van willekeurige code

Windows Standards-Based Storage Management Service:

CVE-ID	CVSS	Impact
CVE-2025-33068	7.50	Denial-of-Service

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2025-29828	8.10	Uitvoeren van willekeurige code

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-32712	7.80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2025-33064	8.80	Uitvoeren van willekeurige code
CVE-2025-33066	8.80	Uitvoeren van willekeurige code

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-33067	8.40	Verkrijgen van verhoogde rechten

Windows Secure Boot:

CVE-ID	CVSS	Impact
CVE-2025-3052	6.70	Omzeilen van beveiligingsmaatregel

Windows Media:

CVE-ID	CVSS	Impact
CVE-2025-32716	7.80	Verkrijgen van verhoogde rechten

Windows Netlogon:

CVE-ID	CVSS	Impact
CVE-2025-33070	8.10	Verkrijgen van verhoogde rechten

Windows SMB:

CVE-ID	CVSS	Impact
CVE-2025-32718	7.80	Verkrijgen van verhoogde rechten
CVE-2025-33073	8.80	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2025-32713	7.80	Verkrijgen van verhoogde rechten

Windows Local Security Authority (LSA):

CVE-ID	CVSS	Impact
CVE-2025-33057	6.50	Denial-of-Service

Microsoft Local Security Authority Server (lsasrv):

CVE-ID	CVSS	Impact
CVE-2025-33056	7.50	Denial-of-Service

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

Windows DHCP Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-32725 | 7.50 | Denial-of-Service                   |
| CVE-2025-33050 | 7.50 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows DWM Core Library:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-33052 | 5.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Shell:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-47160 | 5.40 | 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-2025-29828	8.1 HIGH
CVE-2025-32710	
CVE-2025-32712	

CVE-2025-32713	
CVE-2025-32714	
CVE-2025-32715	6.5 MEDIUM
CVE-2025-32716	
CVE-2025-32718	
CVE-2025-32719	
CVE-2025-32720	
CVE-2025-32721	
CVE-2025-32722	
CVE-2025-32724	
CVE-2025-33058	5.5 MEDIUM
CVE-2025-33059	
CVE-2025-33060	
CVE-2025-33061	
CVE-2025-33062	
CVE-2025-33063	
CVE-2025-33064	
CVE-2025-33065	
CVE-2025-33066	
CVE-2025-33067	8.4 HIGH
CVE-2025-33075	
CVE-2025-47160	
CVE-2025-47955	7.8 HIGH

CVE-2025-33071	8.1 HIGH
CVE-2025-24068	
CVE-2025-24069	
CVE-2025-24065	5.5 MEDIUM
CVE-2025-32725	7.5 HIGH
CVE-2025-33050	7.5 HIGH
CVE-2025-33052	
CVE-2025-33053	
CVE-2025-33055	
CVE-2025-33056	7.5 HIGH
CVE-2025-33057	
CVE-2025-33068	7.5 HIGH
CVE-2025-33070	8.1 HIGH
CVE-2025-33073	
CVE-2025-3052	
CVE-2025-47969	4.4 MEDIUM
CVE-2025-33069	
CVE-2025-47956	

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-822	Untrusted Pointer Dereference

CWE-126	Buffer Over-read
CWE-347	Improper Verification of Cryptographic Signature
CWE-908	Use of Uninitialized Resource
CWE-190	Integer Overflow or Wraparound
CWE-693	Protection Mechanism Failure
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-400	Uncontrolled Resource Consumption
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-73	External Control of File Name or Path
CWE-269	Improper Privilege Management

Getroffen producten

Microsoft
Remote Desktop client for Windows Desktop
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 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 for ARM64-based Systems
Windows 11 Version 24H2 for x64-based Systems
Windows App Client for Windows Desktop

Windows Security App
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)
Windows 10 Version 1507
Windows 10 Version 1607
Windows 10 Version 1809
Windows 10 Version 21H2
Windows 10 Version 22H2
Windows 11 Version 23H2

Windows 11 Version 24H2
Windows 11 version 22H2
Windows 11 version 22H3
Windows Server 2008 Service Pack 2
Windows Server 2008 R2 Service Pack 1
Windows Server 2008 R2 Service Pack 1 (Server Core installation)
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 2008 Service Pack 2
Windows Server 2008 Service Pack 2 (Server Core installation)

Disclaimer