Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0047

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-02-2025

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-Servie (DoS)
- Verkrijgen van verhoogde rechten
- Omzeilen van beveiligingsmaatregel
- Spoofing
- Uitvoer van willekeurige code (Gebruikersrechten)

Van de kwetsbaarheden met kenmerk CVE-2025-21391 en CVE-2025-21418 meldt Microsoft informatie te hebben dat deze beperkt zijn misbruikt. Deze kwetsbaarheden bevinden zich respectievelijk in Windows Storage en WinSOCK. Succesvol misbruik vereist wel dat de kwaadwillende lokale toegang heeft tot het kwetsbare systeem.

Van de kwetsbaarheid met kenmerk CVE-2025-21377 geeft Microsoft aan informatie te hebben dat deze de aandacht heeft van onderzoekers, maar er is (nog) geen publieke Proof-of-Concept (PoC) of exploit bekend. Deze kwetsbaarheid bevindt zich in de wijze waarop omgegaan wordt met NTLMv2.

```
Windows Disk Cleanup Tool:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21420 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Telephony Server:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21201 | 8.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

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

CVE-2025-21349	6.80	<Vertaal: Tampering>

Microsoft Digest Authentication:

CVE-ID	CVSS	Impact
CVE-2025-21368	8.80	Uitvoeren van willekeurige code
CVE-2025-21369	8.80	Uitvoeren van willekeurige code

Windows Internet Connection Sharing (ICS):

CVE-ID	CVSS	Impact
CVE-2025-21352	6.50	Denial-of-Service
CVE-2025-21212	6.50	Denial-of-Service
CVE-2025-21216	6.50	Denial-of-Service
CVE-2025-21254	6.50	Denial-of-Service

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2025-21377	6.50	Voordoen als andere gebruiker

Windows DHCP Client:

CVE-ID	CVSS	Impact
CVE-2025-21179	4.80	Denial-of-Service

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2025-21418	7.80	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2025-21359	7.80	Omzeilen van beveiligingsmaatregel

Windows Win32 Kernel Subsystem:

CVE-ID	CVSS	Impact
CVE-2025-21367	7.80	Verkrijgen van verhoogde rechten

Windows Update Stack:

CVE-ID	CVSS	Impact
CVE-2025-21347	6.00	Denial-of-Service

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2025-21373	7.80	Verkrijgen van verhoogde rechten

Windows Setup Files Cleanup:

CVE-ID	CVSS	Impact
CVE-2025-21419	7.10	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2025-21350	5.90	Denial-of-Service

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

Windows Routing and Remote Access Service (RRAS):

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-21208	8.80	Uitvoeren van willekeurige code
CVE-2025-21410	8.80	Uitvoeren van willekeurige code

Microsoft Streaming Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-21375	7.80	Verkrijgen van verhoogde rechten

Windows CoreMessaging:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-21358	7.80	Verkrijgen van verhoogde rechten
CVE-2025-21184	7.00	Verkrijgen van verhoogde rechten

Windows Resilient File System (ReFS) Deduplication Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-21182	7.40	Verkrijgen van verhoogde rechten
CVE-2025-21183	7.40	Verkrijgen van verhoogde rechten

Windows DHCP Server:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2025-21379	7.10	Uitvoeren van willekeurige code

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2025-21376	8.10	Uitvoeren van willekeurige code

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2025-21406	8.80	Uitvoeren van willekeurige code
CVE-2025-21407	8.80	Uitvoeren van willekeurige code
CVE-2025-21190	8.80	Uitvoeren van willekeurige code
CVE-2025-21200	8.80	Uitvoeren van willekeurige code
CVE-2025-21371	8.80	Uitvoeren van willekeurige code

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2025-21181	7.50	Denial-of-Service

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2025-21414	7.00	Verkrijgen van verhoogde rechten

Microsoft Windows:

CVE-ID	CVSS	Impact
CVE-2025-21337	3.30	Verkrijgen van verhoogde rechten

Windows Storage:

CVE-ID	CVSS	Impact

```
|----------------|------|-------------------------------------|
| CVE-2025-21391 | 7.10 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Active Directory Domain Services:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21351 | 7.50 | Denial-of-Service                   |
|----------------|------|-------------------------------------|
```

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-2025-21351	
CVE-2025-21352	
CVE-2025-21368	
CVE-2025-21369	
CVE-2025-21375	
CVE-2025-21376	
CVE-2025-21391	
CVE-2025-21418	
CVE-2025-21419	
CVE-2025-21420	

- CVE-2025-21407
- CVE-2025-21190
- CVE-2025-21200
- CVE-2025-21201
- CVE-2025-21337
- CVE-2025-21347
- CVE-2025-21349
- CVE-2025-21350
- CVE-2025-21358
- CVE-2025-21367
- CVE-2025-21371
- CVE-2025-21377
- CVE-2025-21184
- CVE-2025-21216
- CVE-2025-21254
- CVE-2025-21414
- CVE-2025-21373
- CVE-2025-21208
- CVE-2025-21410
- CVE-2025-21379
- CVE-2025-21182
- CVE-2025-21183
- CVE-2025-21179

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-822	Untrusted Pointer Dereference
CWE-415	Double Free
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-400	Uncontrolled Resource Consumption
CWE-122	Heap-based Buffer Overflow
CWE-73	External Control of File Name or Path
CWE-20	Improper Input Validation
CWE-287	Improper Authentication

Getroffen producten

microsoft
windows

Disclaimer