Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0434

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-11-2024

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)
- Uitvoer van willekeurige code (Gebruikersrechten)
- Uitvoer van willekeurige code (Systeemrechten)
- Verkrijgen van verhoogde rechten
- Toegang tot gevoelige gegevens
- Spoofing

Van de kwetsbaarheden met kenmerk CVE-2024-43451 en CVE-2024-49019 geeft Microsoft aan signalen te hebben dat informatie gedeeld wordt in diverse groepen.

Van de kwetsbaarheden met kenmerk CVE-2024-43451 en CVE-2024-49039 geeft Microsoft aan dat deze beperkt en gericht zijn misbruikt. Deze kwetsbaarheden bevinden zich respectievelijk in NTLMv2 en de task scheduler en stellen een kwaadwillende in staat zich voor te doen als een andere gebruiker met mogelijk hogere rechten. Succesvol misbruik is niet eenvoudig en vereist dat de kwaadwillende het slachtoffer misleidt een malafide applicatie te draaien.

```
Windows Task Scheduler:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-49039 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Update Stack:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-43530 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows USB Video Driver:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

CVE-2024-43634	6.80	Verkrijgen van verhoogde rechten
CVE-2024-43637	6.80	Verkrijgen van verhoogde rechten
CVE-2024-43638	6.80	Verkrijgen van verhoogde rechten
CVE-2024-43643	6.80	Verkrijgen van verhoogde rechten
CVE-2024-43449	6.80	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2024-43630	7.80	Verkrijgen van verhoogde rechten

Windows Registry:

CVE-ID	CVSS	Impact
CVE-2024-43452	7.50	Verkrijgen van verhoogde rechten
CVE-2024-43641	7.80	Verkrijgen van verhoogde rechten

Microsoft Virtual Hard Drive:

CVE-ID	CVSS	Impact
CVE-2024-38264	5.90	Denial-of-Service

Windows Package Library Manager:

CVE-ID	CVSS	Impact
CVE-2024-38203	6.20	Toegang tot gevoelige gegevens

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact

| CVE-2024-43624 | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2024-43633 | 6.50 | Denial-of-Service |

Windows Defender Application Control (WDAC):

CVE-ID	CVSS	Impact
CVE-2024-43645	6.70	Omzeilen van beveiligingsmaatregel

Windows SMBv3 Client/Server:

CVE-ID	CVSS	Impact
CVE-2024-43447	8.10	Uitvoeren van willekeurige code

Windows VMSwitch:

CVE-ID	CVSS	Impact
CVE-2024-43625	8.10	Verkrijgen van verhoogde rechten

Windows Win32 Kernel Subsystem:

CVE-ID	CVSS	Impact
CVE-2024-49046	7.80	Verkrijgen van verhoogde rechten

Windows CSC Service:

CVE-ID	CVSS	Impact
CVE-2024-43644	7.80	Verkrijgen van verhoogde rechten

Role: Windows Active Directory Certificate Services:

CVE-ID	CVSS	Impact
CVE-2024-49019	7.80	Verkrijgen van verhoogde rechten

Windows SMB:

CVE-ID	CVSS	Impact
CVE-2024-43642	7.50	Denial-of-Service

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2024-43451	6.50	Voordoen als andere gebruiker

Windows NT OS Kernel:

CVE-ID	CVSS	Impact
CVE-2024-43623	7.80	Verkrijgen van verhoogde rechten

Windows DWM Core Library:

CVE-ID	CVSS	Impact
CVE-2024-43629	7.80	Verkrijgen van verhoogde rechten
CVE-2024-43636	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows DNS:

CVE-ID	CVSS	Impact
CVE-2024-43450	7.50	Voordoen als andere gebruiker

Windows Telephony Service:

CVE-ID	CVSS	Impact
CVE-2024-43626	7.80	Verkrijgen van verhoogde rechten
CVE-2024-43627	8.80	Uitvoeren van willekeurige code
CVE-2024-43628	8.80	Uitvoeren van willekeurige code
CVE-2024-43620	8.80	Uitvoeren van willekeurige code
CVE-2024-43621	8.80	Uitvoeren van willekeurige code
CVE-2024-43622	8.80	Uitvoeren van willekeurige code
CVE-2024-43635	8.80	Uitvoeren van willekeurige code

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2024-43639	9.80	Uitvoeren van willekeurige code

Windows Secure Kernel Mode:

CVE-ID	CVSS	Impact
CVE-2024-43631	6.70	Verkrijgen van verhoogde rechten
CVE-2024-43646	6.70	Verkrijgen van verhoogde rechten
CVE-2024-43640	9.80	Uitvoeren van willekeurige code

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-2024-43530	
CVE-2024-43623	
CVE-2024-43625	
CVE-2024-43626	
CVE-2024-43627	
CVE-2024-43628	
CVE-2024-43630	
CVE-2024-43631	
CVE-2024-43634	
CVE-2024-43637	
CVE-2024-43638	
CVE-2024-43643	
CVE-2024-43644	
CVE-2024-43646	
CVE-2024-43447	
CVE-2024-43449	
CVE-2024-43450	
CVE-2024-43451	
CVE-2024-43452	
CVE-2024-49046	
CVE-2024-43620	

- CVE-2024-43621
- CVE-2024-43622
- CVE-2024-43624
- CVE-2024-43629
- CVE-2024-43635
- CVE-2024-43636
- CVE-2024-43639
- CVE-2024-43640
- CVE-2024-43641
- CVE-2024-43642
- CVE-2024-38203
- CVE-2024-49019
- CVE-2024-49039
- CVE-2024-38264
- CVE-2024-43633
- CVE-2024-43645

CWE's

CWE	Beschrijving
CWE-1390	Weak Authentication
CWE-822	Untrusted Pointer Dereference
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-190	Integer Overflow or Wraparound

CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-73	External Control of File Name or Path
CWE-287	Improper Authentication

Getroffen producten

microsoft
windows_10_1507
windows_10_1607
windows_10_1809
windows_10_21h2
windows_10_22h2
windows_11_22h2
windows_11_23h2
windows_11_24h2
windows_server_2008_r2
windows_server_2008_sp2
windows_server_2012
windows_server_2012_r2
windows_server_2016
windows_server_2019
windows_server_2022

windows_server_23h2

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.