Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0392

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-10-2024

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 onderstaande categorieën schade.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2024-38124 toegewezen gekregen en bevindt zich in de NETLOGON functionaliteit. Succesvol misbruik is echter niet eenvoudig en vereist voorafgaande kennis van de infrastructuur en precieze timing, waarbij een randvoorwaarde van succes is dat er een nieuwe Domain Controller wordt ingericht.

Microsoft Simple Certificate Enrollment Protocol:

CVE-ID	CVSS	Impact
CVE-2024-43541	7.50	Denial-of-Service
CVE-2024-43544	7.50	Denial-of-Service

Windows cURL Implementation:

CVE-ID	CVSS	Impact
CVE-2024-6197	8.80	Uitvoeren van willekeurige code,

Windows Secure Channel:

CVE-ID	CVSS	Impact
CVE-2024-43550	7.40	Voordoen als andere gebruiker

Windows Remote Desktop:

CVE-ID	CVSS	Impact
CVE-2024-43582	8.10	Uitvoeren van willekeurige code

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

Microsoft ActiveX:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-43517	8.80	Uitvoeren van willekeurige code

Windows Telephony Server:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-43518	8.80	Uitvoeren van willekeurige code

Windows Remote Desktop Services:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-43456	4.80	Manipuleren van gegevens

Windows MSHTML Platform:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-43573	6.50	Voordoen als andere gebruiker

Windows Mobile Broadband:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-43525	6.80	Uitvoeren van willekeurige code
CVE-2024-43526	6.80	Uitvoeren van willekeurige code
CVE-2024-43537	6.50	Denial-of-Service
CVE-2024-43538	6.50	Denial-of-Service
CVE-2024-43540	6.50	Denial-of-Service
CVE-2024-43542	6.50	Denial-of-Service
CVE-2024-43543	6.80	Uitvoeren van willekeurige code

CVE-2024-43523	6.80	Uitvoeren van willekeurige code
CVE-2024-43524	6.80	Uitvoeren van willekeurige code
CVE-2024-43536	6.80	Uitvoeren van willekeurige code
CVE-2024-43555	6.50	Denial-of-Service
CVE-2024-43557	6.50	Denial-of-Service
CVE-2024-43558	6.50	Denial-of-Service
CVE-2024-43559	6.50	Denial-of-Service
CVE-2024-43561	6.50	Denial-of-Service

Windows Standards-Based Storage Management Service:

CVE-ID	CVSS	Impact
CVE-2024-43512	6.50	Denial-of-Service

Microsoft WDAC OLE DB provider for SQL:

CVE-ID	CVSS	Impact
CVE-2024-43519	8.80	Uitvoeren van willekeurige code

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2024-43533	8.80	Uitvoeren van willekeurige code
CVE-2024-43599	8.80	Uitvoeren van willekeurige code

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact
CVE-2024-43535	7.00	Verkrijgen van verhoogde rechten
CVE-2024-43554	5.50	Toegang tot gevoelige gegevens

Code Integrity Guard:

CVE-ID	CVSS	Impact
CVE-2024-43585	5.50	Omzeilen van beveiligingsmaatregel

Windows Print Spooler Components:

CVE-ID	CVSS	Impact
CVE-2024-43529	7.30	Verkrijgen van verhoogde rechten

Windows Resilient File System (ReFS):

CVE-ID	CVSS	Impact
CVE-2024-43500	5.50	Toegang tot gevoelige gegevens

Microsoft Management Console:

CVE-ID	CVSS	Impact
CVE-2024-43572	7.80	Uitvoeren van willekeurige code

RPC Endpoint Mapper Service:

CVE-ID	CVSS	Impact
CVE-2024-43532	8.80	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2024-43508	5.50	Toegang tot gevoelige gegevens
CVE-2024-43534	6.50	Toegang tot gevoelige gegevens
CVE-2024-43509	7.80	Verkrijgen van verhoogde rechten

| CVE-2024-43556 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Local Security Authority (LSA):

CVE-ID	CVSS	Impact
CVE-2024-43522	7.00	Verkrijgen van verhoogde rechten

Sudo for Windows:

CVE-ID	CVSS	Impact
CVE-2024-43571	5.60	Voordoen als andere gebruiker

Windows Scripting:

CVE-ID	CVSS	Impact
CVE-2024-43584	7.70	Omzeilen van beveiligingsmaatregel

Winlogon:

CVE-ID	CVSS	Impact
CVE-2024-43583	7.80	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2024-38129	7.50	Verkrijgen van verhoogde rechten
CVE-2024-43547	6.50	Toegang tot gevoelige gegevens

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2024-43546	5.60	Toegang tot gevoelige gegevens

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2024-38261	7.80	Uitvoeren van willekeurige code
CVE-2024-43608	8.80	Uitvoeren van willekeurige code
CVE-2024-43607	8.80	Uitvoeren van willekeurige code
CVE-2024-38265	8.80	Uitvoeren van willekeurige code
CVE-2024-43453	8.80	Uitvoeren van willekeurige code
CVE-2024-38212	8.80	Uitvoeren van willekeurige code
CVE-2024-43549	8.80	Uitvoeren van willekeurige code
CVE-2024-43564	8.80	Uitvoeren van willekeurige code
CVE-2024-43589	8.80	Uitvoeren van willekeurige code
CVE-2024-43592	8.80	Uitvoeren van willekeurige code
CVE-2024-43593	8.80	Uitvoeren van willekeurige code
CVE-2024-43611	8.80	Uitvoeren van willekeurige code

Windows EFI Partition:

CVE-ID	CVSS	Impact
CVE-2024-37976	6.70	Omzeilen van beveiligingsmaatregel
CVE-2024-37982	6.70	Omzeilen van beveiligingsmaatregel
CVE-2024-37983	6.70	Omzeilen van beveiligingsmaatregel

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2024-20659	7.10	Omzeilen van beveiligingsmaatregel
CVE-2024-43521	7.50	Denial-of-Service
CVE-2024-43567	7.50	Denial-of-Service
CVE-2024-43575	7.50	Denial-of-Service

Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2024-30092	8.00	Uitvoeren van willekeurige code

Windows NT OS Kernel:

CVE-ID	CVSS	Impact
CVE-2024-43553	7.40	Verkrijgen van verhoogde rechten

Windows Network Address Translation (NAT):

CVE-ID	CVSS	Impact
CVE-2024-43562	7.50	Denial-of-Service
CVE-2024-43565	7.50	Denial-of-Service

Windows Remote Desktop Licensing Service:

CVE-ID	CVSS	Impact
CVE-2024-38262	7.50	Uitvoeren van willekeurige code

OpenSSH for Windows:

CVE-ID	CVSS	Impact
CVE-2024-43581	7.10	Uitvoeren van willekeurige code
CVE-2024-43615	7.10	Uitvoeren van willekeurige code
CVE-2024-38029	7.50	Uitvoeren van willekeurige code

Windows NTFS:

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

CVE-ID	CVSS	Impact
CVE-2024-43514	7.80	Verkrijgen van verhoogde rechten

Windows Netlogon:

CVE-ID	CVSS	Impact
CVE-2024-38124	9.00	Verkrijgen van verhoogde rechten

Windows Storage Port Driver:

CVE-ID	CVSS	Impact
CVE-2024-43560	7.80	Verkrijgen van verhoogde rechten

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2024-43501	7.80	Verkrijgen van verhoogde rechten

Windows Secure Kernel Mode:

CVE-ID	CVSS	Impact
CVE-2024-43516	7.80	Verkrijgen van verhoogde rechten
CVE-2024-43528	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows Speech:

CVE-ID	CVSS	Impact
CVE-2024-43574	8.30	Uitvoeren van willekeurige code

Windows Ancillary Function Driver for WinSock:

CVE-ID	CVSS	Impact
CVE-2024-43563	7.80	Verkrijgen van verhoogde rechten

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2024-43513	6.40	Omzeilen van beveiligingsmaatregel

Windows Online Certificate Status Protocol (OCSP):

CVE-ID	CVSS	Impact
CVE-2024-43545	7.50	Denial-of-Service

Internet Small Computer Systems Interface (iSCSI):

CVE-ID	CVSS	Impact
CVE-2024-43515	7.50	Denial-of-Service

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2024-43502	7.10	Verkrijgen van verhoogde rechten
CVE-2024-43527	7.80	Verkrijgen van verhoogde rechten
CVE-2024-37979	6.70	Verkrijgen van verhoogde rechten
CVE-2024-43511	7.00	Verkrijgen van verhoogde rechten
CVE-2024-43520	5.00	Denial-of-Service
CVE-2024-43570	6.40	Verkrijgen van verhoogde rechten

Azure Stack:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-38179 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows Storage:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-43551 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

Windows Shell:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-43552 | 7.30 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

BranchCache:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-43506 | 7.50 | Denial-of-Service                   |
| CVE-2024-38149 | 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-2024-43516	7.8 HIGH
CVE-2024-43502	7.1 HIGH
CVE-2024-43506	7.5 HIGH
CVE-2024-43513	6.4 MEDIUM
CVE-2024-43515	7.5 HIGH
CVE-2024-43518	8.8 HIGH
CVE-2024-43519	8.8 HIGH
CVE-2024-43525	6.8 MEDIUM
CVE-2024-43526	6.8 MEDIUM
CVE-2024-43532	8.8 HIGH
CVE-2024-43534	6.5 MEDIUM
CVE-2024-43535	7.0 HIGH
CVE-2024-43537	6.5 MEDIUM
CVE-2024-43538	6.5 MEDIUM
CVE-2024-43540	6.5 MEDIUM
CVE-2024-43542	6.5 MEDIUM
CVE-2024-43543	6.8 MEDIUM
CVE-2024-43554	5.5 MEDIUM
CVE-2024-43573	6.5 MEDIUM
CVE-2024-43581	7.1 HIGH
CVE-2024-6197	
CVE-2024-43615	7.1 HIGH
CVE-2024-37976	6.7 MEDIUM

CVE-2024-37982	6.7 MEDIUM
CVE-2024-37983	6.7 MEDIUM
CVE-2024-38149	7.5 HIGH
CVE-2024-43501	7.8 HIGH
CVE-2024-43509	7.8 HIGH
CVE-2024-43511	7.0 HIGH
CVE-2024-43514	7.8 HIGH
CVE-2024-43517	8.8 HIGH
CVE-2024-43520	5.0 MEDIUM
CVE-2024-43523	6.8 MEDIUM
CVE-2024-43524	6.8 MEDIUM
CVE-2024-43528	7.8 HIGH
CVE-2024-43536	6.8 MEDIUM
CVE-2024-43547	6.5 MEDIUM
CVE-2024-43550	7.4 HIGH
CVE-2024-43551	7.8 HIGH
CVE-2024-43553	7.4 HIGH
CVE-2024-43555	6.5 MEDIUM
CVE-2024-43556	7.8 HIGH
CVE-2024-43557	6.5 MEDIUM
CVE-2024-43558	6.5 MEDIUM
CVE-2024-43559	6.5 MEDIUM
CVE-2024-43560	7.8 HIGH

CVE-2024-43561	6.5 MEDIUM
CVE-2024-43562	7.5 HIGH
CVE-2024-43563	7.8 HIGH
CVE-2024-43565	7.5 HIGH
CVE-2024-43570	6.4 MEDIUM
CVE-2024-43572	7.8 HIGH
CVE-2024-43582	8.1 HIGH
CVE-2024-43585	5.5 MEDIUM
CVE-2024-43599	8.8 HIGH
CVE-2024-43583	7.8 HIGH
CVE-2024-20659	7.1 HIGH
CVE-2024-30092	8.0 HIGH
CVE-2024-38261	7.8 HIGH
CVE-2024-43541	7.5 HIGH
CVE-2024-43608	8.8 HIGH
CVE-2024-43607	8.8 HIGH
CVE-2024-37979	6.7 MEDIUM
CVE-2024-38124	9.0 CRITICAL
CVE-2024-38265	8.8 HIGH
CVE-2024-38262	7.5 HIGH
CVE-2024-43453	8.8 HIGH
CVE-2024-38212	8.8 HIGH
CVE-2024-43456	4.8 MEDIUM

CVE-2024-43512	6.5 MEDIUM
CVE-2024-43521	7.5 HIGH
CVE-2024-43544	7.5 HIGH
CVE-2024-43545	7.5 HIGH
CVE-2024-43549	8.8 HIGH
CVE-2024-43564	8.8 HIGH
CVE-2024-43567	7.5 HIGH
CVE-2024-43575	7.5 HIGH
CVE-2024-43589	8.8 HIGH
CVE-2024-43592	8.8 HIGH
CVE-2024-43593	8.8 HIGH
CVE-2024-43611	8.8 HIGH
CVE-2024-43529	7.3 HIGH
CVE-2024-43533	8.8 HIGH
CVE-2024-43546	5.6 MEDIUM
CVE-2024-43574	8.3 HIGH
CVE-2024-43584	7.7 HIGH
CVE-2024-38179	8.8 HIGH
CVE-2024-43508	5.5 MEDIUM
CVE-2024-43500	5.5 MEDIUM
CVE-2024-43522	7.0 HIGH
CVE-2024-43552	7.3 HIGH
CVE-2024-38029	7.5 HIGH

CVE-2024-38129	7.5 HIGH
CVE-2024-43527	7.8 HIGH
CVE-2024-43571	5.6 MEDIUM

CWE's

CWE	Beschrijving
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-197	Numeric Truncation Error
CWE-118	Incorrect Access of Indexable Resource ('Range Error')
CWE-636	Not Failing Securely ('Failing Open')
CWE-590	Free of Memory not on the Heap
CWE-253	Incorrect Check of Function Return Value
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-707	Improper Neutralization
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-908	Use of Uninitialized Resource
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-203	Observable Discrepancy
CWE-325	Missing Cryptographic Step
CWE-190	Integer Overflow or Wraparound

CWE-693	Protection Mechanism Failure
CWE-250	Execution with Unnecessary Privileges
CWE-285	Improper Authorization
CWE-125	Out-of-bounds Read
CWE-862	Missing Authorization
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-73	External Control of File Name or Path
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-20	Improper Input Validation
CWE-287	Improper Authentication
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

microsoft
azure_stack_hci
remote_desktop_client_for_windows_desktop
windows

windows_10_version_1507
windows_10_version_1607
windows_10_version_1809
windows_10_version_21h2
windows_10_version_22h2
windows_11_version_21h2
windows_11_version_22h2
windows_11_version_22h3
windows_11_version_23h2
windows_11_version_24h2
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_service_pack_2
windows_server_2008_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__23h2_edition__server_core_installation_
windows_10

windows_11
windows_server_2008
windows_server_2022_23h2

Disclaimer