Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0279

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-07-2024

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)
- Omzeilen van beveiligingsmaatregel
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- SQL Injection
- Toegang tot systeemgegevens
- Verhoogde gebruikersrechten

De ernstigste kwetsbaarheden hebben kenmerk CVE-2024-38076, CVE-2024-38074 en CVE-2024-38076 toegewezen gekregen en bevindt zich in Windows Remote Desktop Licensing Service. Een ongeauthenticeerde kwaadwillende kan de kwetsbaarheid misbruiken om willekeurige code uit te voeren met verhoogde rechten.

```
---
Windows Server Backup:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-38013 | 6.70 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows PowerShell:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-38043 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2024-38033 | 7.30 | Verkrijgen van verhoogde rechten    |
| CVE-2024-38047 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

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

| CVE-2024-38015 | 7.50 | Denial-of-Service |
| CVE-2024-38076 | 9.80 | Uitvoeren van willekeurige code |

Windows Image Acquisition:

CVE-ID	CVSS	Impact
CVE-2024-38022	7.00	Verkrijgen van verhoogde rechten

Windows Internet Connection Sharing (ICS):

CVE-ID	CVSS	Impact
CVE-2024-38102	6.50	Denial-of-Service
CVE-2024-38053	8.80	Uitvoeren van willekeurige code
CVE-2024-38101	6.50	Denial-of-Service
CVE-2024-38105	6.50	Denial-of-Service

Intel:

CVE-ID	CVSS	Impact
CVE-2024-37985	5.90	Toegang tot gevoelige gegevens

Windows Online Certificate Status Protocol (OCSP):

CVE-ID	CVSS	Impact
CVE-2024-38031	7.50	Denial-of-Service
CVE-2024-38067	7.50	Denial-of-Service
CVE-2024-38068	7.50	Denial-of-Service

Windows COM Session:

| CVE-ID | CVSS | Impact |

| CVE-2024-38100 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2024-38041	5.50	Toegang tot gevoelige gegevens

Windows Secure Boot:

CVE-ID	CVSS	Impact
CVE-2024-28899	8.80	Omzeilen van beveiligingsmaatregel
CVE-2024-37969	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37970	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37974	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37981	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37986	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37987	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-26184	6.80	Omzeilen van beveiligingsmaatregel
CVE-2024-37971	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37972	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37973	7.80	Omzeilen van beveiligingsmaatregel
CVE-2024-37975	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37977	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37978	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37984	8.40	Omzeilen van beveiligingsmaatregel
CVE-2024-37988	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-37989	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-38010	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-38011	8.00	Omzeilen van beveiligingsmaatregel
CVE-2024-38065	6.80	Omzeilen van beveiligingsmaatregel

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact

| CVE-2024-38062 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Win32 Kernel Subsystem:

CVE-ID	CVSS	Impact
CVE-2024-38085	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows Codecs Library:

CVE-ID	CVSS	Impact
CVE-2024-38055	5.50	Toegang tot gevoelige gegevens
CVE-2024-38056	5.50	Toegang tot gevoelige gegevens
CVE-2024-38060	8.80	Uitvoeren van willekeurige code

Windows Workstation Service:

CVE-ID	CVSS	Impact
CVE-2024-38050	7.80	Verkrijgen van verhoogde rechten

Windows LockDown Policy (WLDP):

CVE-ID	CVSS	Impact
CVE-2024-38070	7.80	Omzeilen van beveiligingsmaatregel

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2024-38051	7.80	Uitvoeren van willekeurige code
CVE-2024-38079	7.80	Verkrijgen van verhoogde rechten

Windows MultiPoint Services:

CVE-ID	CVSS	Impact
CVE-2024-30013	8.80	Uitvoeren van willekeurige code

Line Printer Daemon Service (LPD):

CVE-ID	CVSS	Impact
CVE-2024-38027	6.50	Denial-of-Service

NDIS:

CVE-ID	CVSS	Impact
CVE-2024-38048	6.50	Denial-of-Service

Windows CoreMessaging:

CVE-ID	CVSS	Impact
CVE-2024-21417	8.80	Verkrijgen van verhoogde rechten

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact
CVE-2024-30071	4.70	Toegang tot gevoelige gegevens
CVE-2024-30079	7.80	Verkrijgen van verhoogde rechten

Windows Cryptographic Services:

CVE-ID	CVSS	Impact
CVE-2024-30098	7.50	Omzeilen van beveiligingsmaatregel

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

Windows Win32K - GRFX:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-38066	7.80	Verkrijgen van verhoogde rechten

Role: Windows Hyper-V:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-38080	7.80	Verkrijgen van verhoogde rechten

NPS RADIUS Server:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-3596	7.50	Voordoen als andere gebruiker

Microsoft Streaming Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-38054	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38052	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38057	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop Licensing Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-38071	7.50	Denial-of-Service
CVE-2024-38072	7.50	Denial-of-Service
CVE-2024-38077	9.80	Uitvoeren van willekeurige code
CVE-2024-38073	7.50	Denial-of-Service
CVE-2024-38074	9.80	Uitvoeren van willekeurige code

CVE-2024-38099	5.90	Denial-of-Service

Windows NTLM:

CVE-ID	CVSS	Impact
CVE-2024-30081	7.10	Voordoen als andere gebruiker

Microsoft WS-Discovery:

CVE-ID	CVSS	Impact
CVE-2024-38091	7.50	Denial-of-Service

Windows Distributed Transaction Coordinator:

CVE-ID	CVSS	Impact
CVE-2024-38049	6.60	Uitvoeren van willekeurige code

Windows Performance Monitor:

CVE-ID	CVSS	Impact
CVE-2024-38025	7.20	Uitvoeren van willekeurige code
CVE-2024-38019	7.20	Uitvoeren van willekeurige code
CVE-2024-38028	7.20	Uitvoeren van willekeurige code

XBox Crypto Graphic Services:

CVE-ID	CVSS	Impact
CVE-2024-38032	7.10	Uitvoeren van willekeurige code
CVE-2024-38078	7.50	Uitvoeren van willekeurige code

Windows iSCSI:

CVE-ID	CVSS	Impact
CVE-2024-35270	5.30	Denial-of-Service

Windows Enroll Engine:

CVE-ID	CVSS	Impact
CVE-2024-38069	7.00	Omzeilen van beveiligingsmaatregel

Windows Fax and Scan Service:

CVE-ID	CVSS	Impact
CVE-2024-38104	8.80	Uitvoeren van willekeurige code

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2024-38064	7.50	Toegang tot gevoelige gegevens

Windows DHCP Server:

CVE-ID	CVSS	Impact
CVE-2024-38044	7.20	Uitvoeren van willekeurige code

Windows Themes:

CVE-ID	CVSS	Impact
CVE-2024-38030	6.50	Voordoen als andere gebruiker

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2024-38017	5.50	Toegang tot gevoelige gegevens

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2024-38059	7.80	Verkrijgen van verhoogde rechten

Active Directory Rights Management Services:

CVE-ID	CVSS	Impact
CVE-2024-38517	7.80	Verkrijgen van verhoogde rechten
CVE-2024-39684	7.80	Verkrijgen van verhoogde rechten

Windows BitLocker:

CVE-ID	CVSS	Impact
CVE-2024-38058	6.80	Omzeilen van beveiligingsmaatregel

Role: Active Directory Certificate Services; Active Directory Domain Services:

CVE-ID	CVSS	Impact
CVE-2024-38061	7.50	Verkrijgen van verhoogde rechten

Windows Filtering:

CVE-ID	CVSS	Impact

```
|----------------|------|-------------------------------------|
| CVE-2024-38034 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows MSHTML Platform:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-38112 | 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

Dreigingsinformatie

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-21417	
CVE-2024-28899	8.8 HIGH
CVE-2024-30081	7.1 HIGH
CVE-2024-30098	7.5 HIGH
CVE-2024-35270	5.3 MEDIUM
CVE-2024-37969	8.0 HIGH

CVE-2024-37970	8.0 HIGH
CVE-2024-37974	8.0 HIGH
CVE-2024-37981	
CVE-2024-37986	8.0 HIGH
CVE-2024-37987	8.0 HIGH
CVE-2024-38013	6.7 MEDIUM
CVE-2024-38022	7.0 HIGH
CVE-2024-38025	7.2 HIGH
CVE-2024-38034	7.8 HIGH
CVE-2024-38041	
CVE-2024-38043	
CVE-2024-38517	
CVE-2024-38051	7.8 HIGH
CVE-2024-38054	7.8 HIGH
CVE-2024-38055	5.5 MEDIUM
CVE-2024-38056	5.5 MEDIUM
CVE-2024-38060	8.8 HIGH
CVE-2024-38061	7.5 HIGH
CVE-2024-38062	
CVE-2024-38064	7.5 HIGH
CVE-2024-38085	7.8 HIGH
CVE-2024-38091	7.5 HIGH
CVE-2024-38102	6.5 MEDIUM

CVE-2024-38104	8.8 HIGH
CVE-2024-30013	
CVE-2024-30071	4.7 MEDIUM
CVE-2024-30079	7.8 HIGH
CVE-2024-3596	9.0 CRITICAL
CVE-2024-37971	
CVE-2024-37972	
CVE-2024-37973	8.4 HIGH
CVE-2024-37975	
CVE-2024-37984	
CVE-2024-37988	
CVE-2024-37989	8.0 HIGH
CVE-2024-38010	8.0 HIGH
CVE-2024-38011	8.0 HIGH
CVE-2024-38017	
CVE-2024-38019	
CVE-2024-38027	6.5 MEDIUM
CVE-2024-38028	7.2 HIGH
CVE-2024-38030	
CVE-2024-38033	
CVE-2024-38047	
CVE-2024-38048	
CVE-2024-38049	6.6 MEDIUM

CVE-2024-38050	
CVE-2024-38052	
CVE-2024-38053	8.8 HIGH
CVE-2024-38057	7.8 HIGH
CVE-2024-38058	6.8 MEDIUM
CVE-2024-38065	6.8 MEDIUM
CVE-2024-38066	
CVE-2024-38068	
CVE-2024-38069	7.0 HIGH
CVE-2024-38070	
CVE-2024-38079	
CVE-2024-38101	
CVE-2024-38105	6.5 MEDIUM
CVE-2024-39684	
CVE-2024-38015	
CVE-2024-38071	
CVE-2024-38072	
CVE-2024-38077	
CVE-2024-38100	
CVE-2024-38031	
CVE-2024-38044	
CVE-2024-38067	
CVE-2024-38073	

- CVE-2024-38074
- CVE-2024-38076
- CVE-2024-38099
- CVE-2024-38059
- CVE-2024-38080
- CVE-2024-26184
- CVE-2024-37977
- CVE-2024-38032
- CVE-2024-38078
- CVE-2024-37985
- CVE-2024-37978

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-166	Improper Handling of Missing Special Element
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-197	Numeric Truncation Error
CWE-20	Improper Input Validation

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-328	Use of Weak Hash
CWE-347	Improper Verification of Cryptographic Signature
CWE-400	Uncontrolled Resource Consumption
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-668	Exposure of Resource to Wrong Sphere
CWE-674	Uncontrolled Recursion
CWE-693	Protection Mechanism Failure
CWE-73	External Control of File Name or Path
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-908	Use of Uninitialized Resource
CWE-924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel

Getroffen producten

ietf
rfc
microsoft

windows_10_version_1507

Disclaimer