Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0248

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2024
Revisie: 1.0.2

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

Update Revisie 2

Dubbele informatie verwijderd. Producten toegevoegd.

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 kwetsbaarheid heeft kenmerk CVE-2024-30080 toegewezen gekregen en bevindt zich in de MSMQ Message Queueing. Een kwaadwillende kan de kwetsbaarheid misbruiken om willekeurige code uit te voeren met verhoogde rechten. Hiervoor dient de MSMQ wel geactiveerd te zijn. Dit is geen standaard optie. Bij correct gebruik is een actieve MSMQ niet vanaf publieke netwerken te bereiken, maar allen vanaf het lokale netwerk. Grootschalig misbruik is daarmee niet waarschijnlijk.

```
Windows Kernel-Mode Drivers:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-35250 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2024-30084 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Routing and Remote Access Service (RRAS):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-30094 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2024-30095 | 7.80 | Uitvoeren van willekeurige code     |
```

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

Microsoft Windows Speech:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30097	8.80	Uitvoeren van willekeurige code

Windows Standards-Based Storage Management Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30083	7.50	Denial-of-Service

Windows DHCP Server:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30070	7.50	Denial-of-Service

Windows Kernel:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30064	8.80	Verkrijgen van verhoogde rechten
CVE-2024-30068	8.80	Verkrijgen van verhoogde rechten

Microsoft Streaming Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30089	7.80	Verkrijgen van verhoogde rechten
CVE-2024-30090	7.00	Verkrijgen van verhoogde rechten

Windows Remote Access Connection Manager:

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

CVE-ID	CVSS	Impact
CVE-2024-30069	4.70	Toegang tot gevoelige gegevens

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2024-30082	7.80	Verkrijgen van verhoogde rechten
CVE-2024-30087	7.80	Verkrijgen van verhoogde rechten
CVE-2024-30091	7.80	Verkrijgen van verhoogde rechten

Microsoft Windows:

CVE-ID	CVSS	Impact
CVE-2023-50868	7.50	Denial-of-Service

Windows Server Service:

CVE-ID	CVSS	Impact
CVE-2024-30080	9.80	Uitvoeren van willekeurige code
CVE-2024-30062	7.80	Uitvoeren van willekeurige code

Windows Wi-Fi Driver:

CVE-ID	CVSS	Impact
CVE-2024-30078	8.80	Uitvoeren van willekeurige code

Windows Event Logging Service:

CVE-ID	CVSS	Impact
CVE-2024-30072	7.80	Uitvoeren van willekeurige code

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

Windows Container Manager Service:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30076	6.80	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30085	7.80	Verkrijgen van verhoogde rechten

Microsoft WDAC OLE DB provider for SQL:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30077	8.00	Uitvoeren van willekeurige code

Windows Cryptographic Services:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30096	5.50	Toegang tot gevoelige gegevens

Windows NT OS Kernel:

|----------------|------|-------------------------------------|
CVE-ID	CVSS	Impact
CVE-2024-30088	7.00	Verkrijgen van verhoogde rechten
CVE-2024-30099	7.00	Verkrijgen van verhoogde rechten

Winlogon:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |

CVE-2024-30066	5.50	Verkrijgen van verhoogde rechten
CVE-2024-30067	5.50	Verkrijgen van verhoogde rechten

Windows Win32 Kernel Subsystem:

CVE-ID	CVSS	Impact
CVE-2024-30086	7.80	Verkrijgen van verhoogde rechten

Windows Perception Service:

CVE-ID	CVSS	Impact
CVE-2024-35265	7.00	Verkrijgen van verhoogde rechten

Windows Themes:

CVE-ID	CVSS	Impact
CVE-2024-30065	5.50	Denial-of-Service

Windows Storage:

CVE-ID	CVSS	Impact
CVE-2024-30093	7.30	Verkrijgen van verhoogde rechten

Windows Distributed File System (DFS):

CVE-ID	CVSS	Impact
CVE-2024-30063	6.70	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-2024-35265	7.0 HIGH
CVE-2023-50868	
CVE-2024-30062	7.8 HIGH
CVE-2024-30063	6.7 MEDIUM
CVE-2024-30064	8.8 HIGH
CVE-2024-30065	5.5 MEDIUM
CVE-2024-30066	5.5 MEDIUM
CVE-2024-30067	5.5 MEDIUM
CVE-2024-30068	8.8 HIGH
CVE-2024-30069	4.7 MEDIUM
CVE-2024-30070	7.5 HIGH
CVE-2024-30072	7.8 HIGH
CVE-2024-30076	6.8 MEDIUM
CVE-2024-30077	8.0 HIGH
CVE-2024-30078	8.8 HIGH
CVE-2024-30080	9.8 CRITICAL

CVE-2024-30082	7.8 HIGH
CVE-2024-30083	7.5 HIGH
CVE-2024-30084	7.0 HIGH
CVE-2024-30085	7.8 HIGH
CVE-2024-30086	7.8 HIGH
CVE-2024-30087	7.8 HIGH
CVE-2024-30088	7.0 HIGH
CVE-2024-30089	7.8 HIGH
CVE-2024-30090	7.0 HIGH
CVE-2024-30091	7.8 HIGH
CVE-2024-30093	7.3 HIGH
CVE-2024-30094	7.8 HIGH
CVE-2024-30095	7.8 HIGH
CVE-2024-30096	5.5 MEDIUM
CVE-2024-30097	8.8 HIGH
CVE-2024-30099	7.0 HIGH
CVE-2024-35250	7.8 HIGH

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-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-20	Improper Input Validation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-400	Uncontrolled Resource Consumption
CWE-415	Double Free
CWE-416	Use After Free
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-641	Improper Restriction of Names for Files and Other Resources
CWE-822	Untrusted Pointer Dereference

Getroffen producten

microsoft
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_server_2008__service_pack_2
windows_server_2008_r2_service_pack_1__server_core_installation_

windows_server_2008_r2_service_pack_1
windows_server_2008_service_pack_2__server_core_installation_
windows_server_2008_service_pack_2
windows_server_2012__server_core_installation_
windows_server_2012_r2__server_core_installation_
windows_server_2012_r2
windows_server_2012
windows_server_2016__server_core_installation_
windows_server_2016
windows_server_2019__server_core_installation_
windows_server_2019
windows_server_2022__23h2_edition__server_core_installation_

Disclaimer