Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0248

[EMBARGO: Microsoft] Kwetsbaarheden verholpen in Microsoft Windows

2024-06-11 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in Windows.

Interpretaties

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 |

Oplossingen

|----------|------|----------| | 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 |
|----------|------|----------| ```

Dreigingsinformatie

CVE Lijst toe te voegen:

CVE-2023-50868, CVE-2024-30062, CVE-2024-30063, CVE-2024-30064, CVE-2024-30065, CVE-2024-30066, CVE-2024-30067, CVE-2024-30068, CVE-2024-30069, CVE-2024-30070, CVE-2024-30072, CVE-2024-30076, CVE-2024-30077, CVE-2024-30078, CVE-2024-30080, CVE-2024-30082, CVE-2024-30083, CVE-2024-30084, CVE-2024-30085, CVE-2024-30086, CVE-2024-30087, CVE-2024-30088, CVE-2024-30089, CVE-2024-30090, CVE-2024-30091, CVE-2024-30093, CVE-2024-30094, CVE-2024-30095, CVE-2024-30096, CVE-2024-30097, CVE-2024-30099, CVE-2024-35250, CVE-2024-35265