Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0334

Kwetsbaarheden verholpen in Microsoft Windows

2024-08-27 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

Er is Proof-of-Concept-code (PoC) verschenen voor de kwetsbaarheid met kenmerk CVE-2024-38063

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

Microsoft heeft kwetsbaarheden verholpen in Windows. Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service
- Omzeilen van beveiligingsmaatregel
- Manipuleren van gegevens
- Verkrijgen van verhoogde rechten
- Spoofing
- Uitvoeren van willekeurige code (root/administrator rechten)
- Uitvoeren van willekeurige code (Gebruikersrechten)
- Toegang tot systeemgegevens

Van de kwetsbaarheden met kenmerk CVE-2024-38106, CVE-2024-38107, CVE-2024-38178 en CVE-2024-38193 geeft Microsoft aan informatie te hebben dat deze actief zijn misbruikt.

De kwetsbaarheden met kenmerk CVE-2024-38106, CVE-2024-38107 en CVE-2024-38193 bevinden zich respectievelijk in de Kernel, de Power Dependency Coördinator en de Ancillary Function Driver for WinSock en stellen een lokale, geauthenticeerde kwaadwillende in staat om zich verhoogde rechten toe te kennen en code uit te voeren met SYSTEM rechten.

De kwetsbaarheid met kenmerk CVE-2024-38178 bevindt zich in de Scripting Engine en stelt een kwaadwillende in staat om willekeurige code uit te voeren met rechten van het slachtoffer. Succesvol misbruik vereist wel dat de kwaadwillende het slachtoffer misleidt om de Edge browser in 'Internet Explorer mode' laat draaien. Van de genoemde kwetsbaarheden is geen publieke Proof-of-Concept-code of exploit beschikbaar. Het vermoeden van het NCSC is echter dat deze wel op korte termijn publiek beschikbaar zal komen. Grootschalig actief misbruik is minder waarschijnlijk, vanwege de beperkende voorwaarden van misbruik.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2024-38063 toegewezen gekregen en bevindt zich in de wijze waarop Windows het IPv6 Protocol verwerkt. Een kwaadwillende kan zonder voorafgaande authenticatie op afstand willekeurige code uitvoeren op het kwetsbare systeem door het herhaaldelijk verzenden van speciaal geprepareerde IPv6 packets. IPv6 is standaard actief. Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd waarmee de kwetsbaarheid kan worden aangetoond. De PoC code vereist dat het doelwit onder controle is van de onderzoeker en veroorzaakt op dit moment hooguit een memory corruption wat resulteert in een crash van het systeem. Uitvoer van willekeurige code wordt niet bereikt. De kans op grootschalig misbruik wordt hiermee groter, maar door de beperkende voorwaarde om de PoC werkend te krijgen is deze

PoC niet zondermeer grootschalig op internet in te zetten. Microsoft is niet op de hoogte dat de kwetsbaarheid actief wordt misbruikt. Microsoft adviseert om als mitigerende maatregel IPv6 uit te schakelen indien dit niet strikt noodzakelijk is.

Oplossingen

De kwetsbaarheden met kenmerk CVE-2024-21302 en CVE-2024-38202 zijn op de laatste BlackHat Conference gepubliceerd door de onderzoeker die ze ontdekt heeft. Deze kwetsbaarheden worden in de gegevens van deze maandelijkse update wel genoemd, maar in deze update worden ze niet verholpen. Microsoft geeft aan nog aan een oplossing te werken en heeft wel mitigerende maatregelen gepubliceerd, om de dreiging van misbruik zo goed als mogelijk te beperken. Zie hiervoor de referenties naar de specifieke kwetsbaarheid.

De kwetsbaarheden stellen een kwaadwillende in staat om een roll-back uit te voeren van geïnstalleerde updates en zo het systeem weer kwetsbaar te maken voor oudere kwetsbaarheden, zonder dat dit ontdekt kan worden door het systeem. Voor het slachtoffer blijft het systeem voldoen aan de laatste beveiligingsupdates. Succesvol misbruik is niet eenvoudig en vereist dat de kwaadwillende over verhoogde rechten beschikt op het kwetsbare systeem. Actief misbruik zal dus vermoedelijk een volgende stap in een keten zijn door een kwaadwillende die op andere wijze toegang heeft gekregen tot het kwetsbare systeem en deze kwetsbaarheden gebruikt om permanente toegang te garanderen.

``` Windows Mark of the Web (MOTW):
|----------|------|----------| | CVE-ID | CVSS | Impact |
|----------|------|----------| | CVE-2024-38213 | 6.50 |
Omzeilen van beveiligingsmaatregel |
|----------|------|----------|

Windows Compressed Folder:
|----------|------|----------| | CVE-ID | CVSS | Impact |
|----------|------|----------| | CVE-2024-38165 | 6.50 |
Manipuleren van gegevens | |----------|------|----------|

Windows Update Stack: |----------|------|----------| |
CVE-ID | CVSS | Impact | |----------|------|----------| |
CVE-2024-38163 | 7.80 | Verkrijgen van verhoogde rechten | |
CVE-2024-38202 | 7.30 | Verkrijgen van verhoogde rechten |
|----------|------|----------|

Microsoft Windows DNS: |----------|------|----------| |
CVE-ID | CVSS | Impact | |----------|------|----------| |
CVE-2024-37968 | 7.50 | Voordoen als andere gebruiker |
|----------|------|----------|

Windows Mobile Broadband: |----------|------|----------|
| CVE-ID | CVSS | Impact | |----------|------|----------| |
CVE-2024-38161 | 6.80 | Uitvoeren van willekeurige code |
|----------|------|----------|

Windows Ancillary Function Driver for WinSock:
|----------|------|----------| | CVE-ID | CVSS | Impact |
|----------|------|----------| | CVE-2024-38193 | 7.80 |
```

Verkrijgen van verhoogde rechten | | CVE-2024-38141 | 7.80 | Verkrijgen van verhoogde rechten | |----------|------|----------------------------------|

Windows IP Routing Management Snapin:
|----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38114 | 8.80 | Uitvoeren van willekeurige code | | CVE-2024-38115 | 8.80 | Uitvoeren van willekeurige code | | CVE-2024-38116 | 8.80 | Uitvoeren van willekeurige code | |----------|------|----------------------------------|

Windows Kernel: |----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38106 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2024-38127 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38133 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38151 | 5.50 | Toegang tot gevoelige gegevens | | CVE-2024-38153 | 7.80 | Verkrijgen van verhoogde rechten | |----------|------|----------------------------------|

Windows Secure Boot: |----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2022-2601 | 8.60 | Omzeilen van beveiligingsmaatregel | | CVE-2023-40547 | 8.30 | Omzeilen van beveiligingsmaatregel | | CVE-2022-3775 | 7.10 | Uitvoeren van willekeurige code | |----------|------|----------------------------------|

Windows Kernel-Mode Drivers:
|----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38184 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38191 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38185 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38186 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38187 | 7.80 | Verkrijgen van verhoogde rechten | |----------|------|----------------------------------|

Windows Print Spooler Components:
|----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38198 | 7.50 | Verkrijgen van verhoogde rechten | |----------|------|----------------------------------|

Windows Power Dependency Coordinator:
|----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38107 | 7.80 | Verkrijgen van verhoogde rechten | |----------|------|----------------------------------|

Windows SmartScreen: |----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38180 | 8.80 | Uitvoeren van willekeurige code | |----------|------|----------------------------------|

Windows Initial Machine Configuration:
|----------|------|----------------------------------| | CVE-ID | CVSS | Impact | |----------|------|----------------------------------| | CVE-2024-38223 | 6.80 |

Verkrijgen van verhoogde rechten |
|---|---|---|

Line Printer Daemon Service (LPD):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38199 | 9.80 |
Uitvoeren van willekeurige code |
|---|---|---|

Microsoft Streaming Service:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38125 | 7.80 |
Verkrijgen van verhoogde rechten | | CVE-2024-38134 | 7.80 | Verkrijgen
van verhoogde rechten | | CVE-2024-38144 | 8.80 | Verkrijgen van
verhoogde rechten | |---|---|---|

Windows Kerberos: |---|---|---| | CVE-ID
| CVSS | Impact | |---|---|---| |
CVE-2024-29995	8.10	Verkrijgen van verhoogde rechten

Windows Security Center: |---|---|---| |
CVE-ID | CVSS | Impact | |---|---|---| |
CVE-2024-38155	5.50	Toegang tot gevoelige gegevens

Windows Scripting: |---|---|---| | CVE-ID
| CVSS | Impact | |---|---|---| |
CVE-2024-38178	7.50	Uitvoeren van willekeurige code

Microsoft Local Security Authority Server (lsasrv):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38118 | 5.50 |
Toegang tot gevoelige gegevens | | CVE-2024-38122 | 5.50 | Toegang tot
gevoelige gegevens | |---|---|---|

Windows NTFS: |---|---|---| | CVE-ID |
CVSS | Impact | |---|---|---| |
CVE-2024-38117	7.80	Verkrijgen van verhoogde rechten

Windows Routing and Remote Access Service (RRAS):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38121 | 8.80 |
Uitvoeren van willekeurige code | | CVE-2024-38128 | 8.80 | Uitvoeren
van willekeurige code | | CVE-2024-38130 | 8.80 | Uitvoeren van
willekeurige code | | CVE-2024-38154 | 8.80 | Uitvoeren van willekeurige
code | | CVE-2024-38120 | 8.80 | Uitvoeren van willekeurige code | |
CVE-2024-38214	6.50	Toegang tot gevoelige gegevens

Windows WLAN Auto Config Service:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38143 | 4.20 |

Verkrijgen van verhoogde rechten |
|---|---|---|

Referenties

Windows NT OS Kernel: |---|---|---| |
CVE-ID | CVSS | Impact | |---|---|---| |
CVE-2024-38135	7.80	Verkrijgen van verhoogde rechten

Windows Network Address Translation (NAT):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38126 | 7.50 |
Denial-of-Service | | CVE-2024-38132 | 7.50 | Denial-of-Service |
|---|---|---|

Windows Resource Manager:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38136 | 7.00 |
Verkrijgen van verhoogde rechten | | CVE-2024-38137 | 7.00 | Verkrijgen
van verhoogde rechten | |---|---|---|

Windows Common Log File System Driver:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38196 | 7.80 |
Verkrijgen van verhoogde rechten |
|---|---|---|

Windows Transport Security Layer (TLS):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38148 | 7.50 |
Denial-of-Service | |---|---|---|

Windows Secure Kernel Mode:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-21302 | 6.70 |
Verkrijgen van verhoogde rechten | | CVE-2024-38142 | 7.80 | Verkrijgen
van verhoogde rechten | |---|---|---|

Reliable Multicast Transport Driver (RMCAST):
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38140 | 9.80 |
Uitvoeren van willekeurige code |
|---|---|---|

Microsoft Bluetooth Driver: |---|---|---| |
CVE-ID | CVSS | Impact | |---|---|---| |
CVE-2024-38123	4.40	Toegang tot gevoelige gegevens

Windows TCP/IP: |---|---|---| | CVE-ID |
CVSS | Impact | |---|---|---| |
CVE-2024-38063	9.80	Uitvoeren van willekeurige code

Windows Cloud Files Mini Filter Driver:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38215 | 7.80 |

Verkrijgen van verhoogde rechten |
|---|---|---|

Windows DWM Core Library: |---|---|---|
| CVE-ID | CVSS | Impact | |---|---|---| |
CVE-2024-38147 | 7.80 | Verkrijgen van verhoogde rechten | |
CVE-2024-38150	7.80	Verkrijgen van verhoogde rechten

Windows Clipboard Virtual Channel Extension:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38131 | 8.80 |
Uitvoeren van willekeurige code |
|---|---|---|

Windows Network Virtualization:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38159 | 9.10 |
Uitvoeren van willekeurige code | | CVE-2024-38160 | 9.10 | Uitvoeren
van willekeurige code | |---|---|---|

Windows Deployment Services:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38138 | 7.50 |
Uitvoeren van willekeurige code |
|---|---|---|

Microsoft WDAC OLE DB provider for SQL:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38152 | 7.80 |
Uitvoeren van willekeurige code |
|---|---|---|

Windows Layer-2 Bridge Network Driver:
|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---| | CVE-2024-38145 | 7.50 |
Denial-of-Service | | CVE-2024-38146 | 7.50 | Denial-of-Service |
|---|---|---| ```

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202