Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0363

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-09-2024

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 een Denial-of-Service te veroorzaken, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren met rechten van het slachtoffer en mogelijk toegang te krijgen tot gevoelige gegevens.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2024-43491 toegewezen gekregen en bevindt zich in het update-mechanisme van Windows. Door een fout in een vorige Services Stack Update (SSU) bleken eerder verholpen kwetsbaarheden weer te zijn teruggedraaid. Een of meer van deze kwetsbaarheden zijn vervolgens misbruikt door kwaadwillenden. Uitsluitend Windows 10 build 1507 installaties die de security updates vanaf maart 2024 (KB5035858), of andere updates t/m augustus 2024 hebben geïnstalleerd zijn kwetsbaar. Microsoft heeft geen informatie vrijgegeven om welke kwetsbaarheden dit precies gaat, maar adviseert om achtereenvolgens de September 2024 Servicing stack update (SSU KB5043936) EN de September 2024 Windows security update (KB5043083) te installeren. Meer detailinformatie kan worden verkregen in de Security Guidance van deze specifieke kwetsbaarheid. Zie hiervoor de bijgevoegde referenties.

Van de kwetsbaarheden met kenmerk CVE-2024-38014 en CVE-2024-38217 geeft Microsoft aan informatie te hebben dat deze beperkt en gericht zijn misbruikt. De kwetsbaarheid met kenmerk CVE-2024-38014 bevindt zich in de Installer en stelt een lokale kwaadwillende in staat zich verhoogde rechten toe te kennen, mogelijk tot SYSTEM-niveau. De kwetsbaarheid met kenmerk CVE-2024-38217 bevindt zich in de Mark of the Web functionaliteit en stelt een kwaadwillende in staat om Mark of the Web te omzeilen en zo malafide code te (laten) uitvoeren door het slachtoffer. Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bestand te downloaden en uit te voeren vanaf een webserver onder controle van de kwaadwillende. Van de kwetsbaarheid met kenmerk CVE-2024-38217 geeft Microsoft aan bekend te zijn dat Proof-of-Concept-code wordt gedeeld binnen gesloten gemeenschappen. Van de kwetsbaarheid met kenmerk CVE-2024-38014 is (nog) geen Proof-of-Concept-code bekend.

```
Windows Kernel-Mode Drivers:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2024-38256 | 5.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Mark of the Web (MOTW):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
```

| CVE-2024-38217 | 5.40 | Omzeilen van beveiligingsmaatregel |
| CVE-2024-43487 | 6.50 | Omzeilen van beveiligingsmaatregel |

Windows MSHTML Platform:

CVE-ID	CVSS	Impact
CVE-2024-43461	8.80	Voordoen als andere gebruiker

Windows AllJoyn API:

CVE-ID	CVSS	Impact
CVE-2024-38257	7.50	Toegang tot gevoelige gegevens

Windows Standards-Based Storage Management Service:

CVE-ID	CVSS	Impact
CVE-2024-38230	6.50	Denial-of-Service

Windows Security Zone Mapping:

CVE-ID	CVSS	Impact
CVE-2024-30073	7.80	Omzeilen van beveiligingsmaatregel

Windows Remote Access Connection Manager:

CVE-ID	CVSS	Impact
CVE-2024-38240	8.10	Verkrijgen van verhoogde rechten

Windows Update:

CVE-ID	CVSS	Impact
CVE-2024-43491	9.80	Uitvoeren van willekeurige code

Windows Installer:

CVE-ID	CVSS	Impact
CVE-2024-38014	7.80	Verkrijgen van verhoogde rechten

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2024-38249	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38250	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38247	7.80	Verkrijgen van verhoogde rechten

Windows Libarchive:

CVE-ID	CVSS	Impact
CVE-2024-43495	7.30	Uitvoeren van willekeurige code

Windows Setup and Deployment:

CVE-ID	CVSS	Impact
CVE-2024-43457	7.80	Verkrijgen van verhoogde rechten

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2024-38239	7.20	Verkrijgen van verhoogde rechten

Windows Authentication Methods:

CVE-ID	CVSS	Impact
CVE-2024-38254	5.50	Toegang tot gevoelige gegevens

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2024-38246	7.00	Verkrijgen van verhoogde rechten

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2024-38235	6.50	Denial-of-Service

Windows PowerShell:

CVE-ID	CVSS	Impact
CVE-2024-38046	7.80	Verkrijgen van verhoogde rechten

Microsoft Streaming Service:

CVE-ID	CVSS	Impact
CVE-2024-38241	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38242	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38237	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38238	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38243	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38244	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38245	7.80	Verkrijgen van verhoogde rechten

Windows Network Address Translation (NAT):

CVE-ID	CVSS	Impact
CVE-2024-38119	7.50	Uitvoeren van willekeurige code

Windows Remote Desktop Licensing Service:

CVE-ID	CVSS	Impact
CVE-2024-43467	7.50	Uitvoeren van willekeurige code
CVE-2024-38231	6.50	Denial-of-Service
CVE-2024-38258	6.50	Toegang tot gevoelige gegevens
CVE-2024-38260	8.80	Uitvoeren van willekeurige code
CVE-2024-38263	7.50	Uitvoeren van willekeurige code
CVE-2024-43454	7.10	Uitvoeren van willekeurige code
CVE-2024-43455	8.80	Voordoen als andere gebruiker

Windows Win32K - ICOMP:

CVE-ID	CVSS	Impact
CVE-2024-38252	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38253	7.80	Verkrijgen van verhoogde rechten

Windows TCP/IP:

CVE-ID	CVSS	Impact
CVE-2024-21416	8.10	Uitvoeren van willekeurige code
CVE-2024-38045	8.10	Uitvoeren van willekeurige code

Windows DHCP Server:

CVE-ID	CVSS	Impact

CVE-2024-38236	7.50	Denial-of-Service

Windows Network Virtualization:

CVE-ID	CVSS	Impact
CVE-2024-38232	7.50	Denial-of-Service
CVE-2024-38233	7.50	Denial-of-Service
CVE-2024-38234	6.50	Denial-of-Service
CVE-2024-43458	7.70	Toegang tot gevoelige gegevens

Windows Storage:

CVE-ID	CVSS	Impact
CVE-2024-38248	7.00	Verkrijgen van verhoogde rechten

Microsoft Management Console:

CVE-ID	CVSS	Impact
CVE-2024-38259	8.80	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

Referenties

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-38230	6.5 MEDIUM
CVE-2024-38236	7.5 HIGH
CVE-2024-38240	
CVE-2024-38241	7.8 HIGH
CVE-2024-38242	
CVE-2024-38249	
CVE-2024-38250	7.8 HIGH
CVE-2024-38252	
CVE-2024-38254	
CVE-2024-38256	5.5 MEDIUM
CVE-2024-43467	
CVE-2024-38014	
CVE-2024-38046	
CVE-2024-38217	
CVE-2024-38231	
CVE-2024-38234	
CVE-2024-38235	
CVE-2024-38237	7.8 HIGH
CVE-2024-38238	
CVE-2024-38239	
CVE-2024-38243	7.8 HIGH

CVE-2024-38244	
CVE-2024-38245	7.8 HIGH
CVE-2024-38247	
CVE-2024-38257	
CVE-2024-38258	6.5 MEDIUM
CVE-2024-38260	
CVE-2024-38263	7.5 HIGH
CVE-2024-21416	
CVE-2024-38045	
CVE-2024-38119	
CVE-2024-43454	
CVE-2024-43455	
CVE-2024-43461	
CVE-2024-30073	
CVE-2024-43487	6.5 MEDIUM
CVE-2024-38246	7.0 HIGH
CVE-2024-38248	7.0 HIGH
CVE-2024-38259	
CVE-2024-38232	
CVE-2024-38233	7.5 HIGH
CVE-2024-43458	7.7 HIGH
CVE-2024-38253	7.8 HIGH
CVE-2024-43495	7.3 HIGH

CVE-2024-43457	
CVE-2024-43491	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-591	Sensitive Data Storage in Improperly Locked Memory
CWE-1390	Weak Authentication
CWE-126	Buffer Over-read
CWE-41	Improper Resolution of Path Equivalence
CWE-415	Double Free
CWE-908	Use of Uninitialized Resource
CWE-23	Relative Path Traversal
CWE-190	Integer Overflow or Wraparound
CWE-693	Protection Mechanism Failure
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-285	Improper Authorization
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-428	Unquoted Search Path or Element
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-400	Uncontrolled Resource Consumption
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-269	Improper Privilege Management

CWE-20	Improper Input Validation

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_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_

Disclaimer