Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0251

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2025

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, waaronder Hyper-V, Graphics Component, en Routing and Remote Access Service (RRAS).

Duiding

De kwetsbaarheden omvatten verschillende soorten aanvallen, zoals lokale privilege-escalatie, onterecht toegang tot gevoelige informatie, en de mogelijkheid voor ongeautoriseerde code-uitvoering. ``` Windows Security App: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53769 | 5.50 | Voordoen als andere gebruiker | |----------------|------|-----------------------------------| Windows StateRepository API: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53789 | 7.80 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Windows Win32K - GRFX: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-50161 | 7.30 | Verkrijgen van verhoogde rechten | | CVE-2025-53132 | 8.00 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Desktop Windows Manager: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-50153 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53152 | 7.80 | Uitvoeren van willekeurige code | |----------------|------|-----------------------------------| Graphics Kernel: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-50176 | 7.80 | Uitvoeren van willekeurige code | |----------------|------|-----------------------------------| Windows NTLM: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53778 | 8.80 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Windows Ancillary Function Driver for WinSock: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-49762 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2025-53134 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2025-53137 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2025-53141 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53147 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2025-53154 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53718 | 7.00 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Windows Kernel: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-49761 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53151 | 7.80 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Storage Port Driver: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53156 | 5.50 | Toegang tot gevoelige gegevens | |----------------|------|-----------------------------------| Kernel Transaction Manager: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53140 | 7.00 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------| Microsoft Brokering File System: |----------------|------|-----------------------------------| | CVE-ID | CVSS | Impact | |----------------|------|-----------------------------------| | CVE-2025-53142 | 7.00 | Verkrijgen van verhoogde rechten | |----------------|------|-----------------------------------|

Windows Connected Devices Platform Service: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-53721 | 7.00 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows Installer: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-50173 | 7.80 | Verkrijgen van verhoogde rechten | |---|---|---|
Microsoft Graphics Component: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-49743 | 6.70 | Verkrijgen van verhoogde rechten | | CVE-2025-50165 | 9.80 | Uitvoeren van willekeurige code | |---|---|---|
Remote Desktop Server: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-50171 | 9.10 | Voordoen als andere gebruiker | |---|---|---|
Windows Kerberos: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-53779 | 7.20 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows Routing and Remote Access Service (RRAS): |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-49757 | 8.80 | Uitvoeren van willekeurige code | | CVE-2025-50156 | 5.70 | Toegang tot gevoelige gegevens | | CVE-2025-50160 | 8.00 | Uitvoeren van willekeurige code | | CVE-2025-50162 | 8.00 | Uitvoeren van willekeurige code | | CVE-2025-50163 | 8.80 | Uitvoeren van willekeurige code | | CVE-2025-50164 | 8.00 | Uitvoeren van willekeurige code | | CVE-2025-53138 | 5.70 | Toegang tot gevoelige gegevens | | CVE-2025-53148 | 5.70 | Toegang tot gevoelige gegevens | | CVE-2025-53153 | 5.70 | Toegang tot gevoelige gegevens | | CVE-2025-53719 | 5.70 | Toegang tot gevoelige gegevens | | CVE-2025-53720 | 8.00 | Uitvoeren van willekeurige code | | CVE-2025-50157 | 5.70 | Toegang tot gevoelige gegevens | |---|---|---|
Windows NTFS: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-50158 | 7.00 | Toegang tot gevoelige gegevens | |---|---|---|
Role: Windows Hyper-V: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-49751 | 6.80 | Denial-of-Service | | CVE-2025-50167 | 7.00 | Verkrijgen van verhoogde rechten | | CVE-2025-53155 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53723 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-48807 | 7.50 | Uitvoeren van willekeurige code | |---|---|---|
Windows NT OS Kernel: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-53136 | 5.50 | Toegang tot gevoelige gegevens | |---|---|---|
Windows PrintWorkflowUserSvc: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-53133 | 7.80 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows Push Notifications: |---|---|---| | CVE-ID | CVSS | Impact | |---|---|---| | CVE-2025-53724 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53725 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-53726 |

Oplossingen

7.80 | Verkrijgen van verhoogde rechten | | CVE-2025-50155 | 7.80 | Verkrijgen van verhoogde rechten |
|---|---|---|
Windows File Explorer: |---|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---|---| | CVE-2025-50154 | 7.50 | Voordoen als andere gebruiker | |---|---|---|
Windows Remote Desktop Services: |---|---|---|---| | CVE-ID | CVSS | Impact | |---|---|---|---| | CVE-2025-53722 | 7.50 | Denial-of-Service | |---|---|---|
Windows Media: |---|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---|---| | CVE-2025-53131 | 8.80 | Uitvoeren van willekeurige code | |---|---|---|
Windows Distributed Transaction Coordinator: |---|---|---|---| | CVE-ID | CVSS | Impact | |---|---|---|---| | CVE-2025-50166 | 6.50 | Toegang tot gevoelige gegevens | |---|---|---|
Windows SMB: |---|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---|---| | CVE-2025-50169 | 7.50 | Uitvoeren van willekeurige code | |---|---|---|
Kernel Streaming WOW Thunk Service Driver: |---|---|---|---| | CVE-ID | CVSS | Impact | |---|---|---|---| | CVE-2025-53149 | 7.80 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows Cloud Files Mini Filter Driver: |---|---|---|---| | CVE-ID | CVSS | Impact | |---|---|---|---| | CVE-2025-50170 | 7.80 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows DirectX: |---|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---|---| | CVE-2025-50172 | 6.50 | Denial-of-Service | | CVE-2025-53135 | 7.00 | Verkrijgen van verhoogde rechten |
|---|---|---|
Remote Access Point-to-Point Protocol (PPP) EAP-TLS:
|---|---|---|---| | CVE-ID | CVSS | Impact |
|---|---|---|---| | CVE-2025-50159 | 7.30 | Verkrijgen van verhoogde rechten | |---|---|---|
Windows Local Security Authority Subsystem Service (LSASS):
|---|---|---|---| | CVE-ID | CVSS | Impact |
---|---|---|---|	CVE-2025-53716	6.50	Denial-of-Service
Windows GDI+: |---|---|---|---|	CVE-ID	CVSS	Impact
---|---|---|---|	CVE-2025-53766	9.80	Uitvoeren van willekeurige code	|---|---|---
Windows Message Queuing: |---|---|---|---| | CVE-ID | CVSS | Impact | |---|---|---|---| | CVE-2025-50177 | 8.10 | Uitvoeren van willekeurige code | | CVE-2025-53143 | 8.80 | Uitvoeren van willekeurige code | | CVE-2025-53144 | 8.80 | Uitvoeren van willekeurige code | | CVE-2025-53145 | 8.80 | Uitvoeren van willekeurige code |
|---|---|---|

Microsoft heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Windows Win32K - ICOMP: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2025-50168 | 7.80 | Verkrijgen van verhoogde rechten | |----------|------|----------| ```

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-48807	
CVE-2025-49743	6.7 MEDIUM
CVE-2025-49751	
CVE-2025-49757	8.8 HIGH
CVE-2025-49761	7.8 HIGH
CVE-2025-49762	7.0 HIGH
CVE-2025-50153	7.8 HIGH
CVE-2025-50154	7.5 HIGH
CVE-2025-50155	7.8 HIGH
CVE-2025-50156	5.7 MEDIUM
CVE-2025-50157	
CVE-2025-50158	7.0 HIGH
CVE-2025-50159	7.3 HIGH
CVE-2025-50160	
CVE-2025-50161	
CVE-2025-50162	
CVE-2025-50163	8.8 HIGH
CVE-2025-50164	8.0 HIGH
CVE-2025-50165	9.8 CRITICAL
CVE-2025-50166	6.5 MEDIUM
CVE-2025-50167	7.0 HIGH

CVE-2025-50168	
CVE-2025-50169	
CVE-2025-50170	7.8 HIGH
CVE-2025-50171	
CVE-2025-50172	
CVE-2025-50173	
CVE-2025-50176	7.8 HIGH
CVE-2025-50177	
CVE-2025-53131	
CVE-2025-53132	8.0 HIGH
CVE-2025-53133	
CVE-2025-53134	
CVE-2025-53135	
CVE-2025-53136	
CVE-2025-53137	
CVE-2025-53138	5.7 MEDIUM
CVE-2025-53140	
CVE-2025-53141	
CVE-2025-53142	7.0 HIGH
CVE-2025-53143	
CVE-2025-53144	
CVE-2025-53145	
CVE-2025-53147	7.0 HIGH

CVE-2025-53148	
CVE-2025-53149	7.8 HIGH
CVE-2025-53151	
CVE-2025-53152	
CVE-2025-53153	5.7 MEDIUM
CVE-2025-53154	
CVE-2025-53155	7.8 HIGH
CVE-2025-53156	
CVE-2025-53716	
CVE-2025-53718	
CVE-2025-53719	
CVE-2025-53720	8.0 HIGH
CVE-2025-53721	7.0 HIGH
CVE-2025-53722	
CVE-2025-53723	
CVE-2025-53724	
CVE-2025-53725	7.8 HIGH
CVE-2025-53726	
CVE-2025-53766	9.8 CRITICAL
CVE-2025-53769	
CVE-2025-53778	8.8 HIGH
CVE-2025-53779	
CVE-2025-53789	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-197	Numeric Truncation Error
CWE-820	Missing Synchronization
CWE-1390	Weak Authentication
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-822	Untrusted Pointer Dereference
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-415	Double Free
CWE-908	Use of Uninitialized Resource
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-23	Relative Path Traversal
CWE-190	Integer Overflow or Wraparound
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-125	Out-of-bounds Read
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-73	External Control of File Name or Path

CWE-287	Improper Authentication

Getroffen producten

Microsoft
Windows 10 Version 22H2
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 11 21h2
Windows 11 22H2