Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0353

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2026
Revisie: 1.0.1

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 1

Microsoft heeft 2 zeroday-kwetsbaarheden in Windows verholpen. Deze zijn aan deze advisory toegevoegd.

Feiten

Microsoft heeft 666 kwetsbaarheden verholpen in Windows.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade, zoals genoemd in onderstaande tabel.

Microsoft heeft voor Windows 666 kwetsbaarheden verholpen. De 32 ernstigste kwetsbaarheden bevinden zich in meerdere Windows componenten en hebben een CVSS score van 9.0 en hoger toegewezen gekregen. Kwaadwillenden met toegang tot deze componenten kunnen zonder voorafgaande authenticatie mogelijk code uitvoeren of zich toegang verschaffen tot het kwetsbare systeem. Deze kwetsbaarheden zijn in onderstaande tabel weergegeven.

De overige 634 kwetsbaarheden variëren in ernst van middelmatig tot hoog en kritiek. Raapleeg het MSRC-portaal voor aanvullende informatie.

==**UPDATE**==

De kwetsbaarheid met kenmerk CVE-2026-81963 heeft een CVSS-score van 7,8. Het betreft een privilege-escalatiekwetsbaarheid in de Windows Update Stack. Een geauthenticeerde kwaadwillende kan deze kwetsbaarheid lokaal misbruiken om zijn rechten te verhogen en SYSTEM-rechten te verkrijgen. Microsoft meldt dat de kwetsbaarheid actief wordt misbruikt. Er zijn geen details bekend over de wijze waarop de kwetsbaarheid bij aanvallen wordt misbruikt.

De kwetsbaarheid met kenmerk CVE-2026-85880 heeft een CVSS-score van 7,8. Het betreft een privilege-escalatiekwetsbaarheid in Windows Advanced Local Procedure Call (ALPC). Een geauthenticeerde kwaadwillende kan deze kwetsbaarheid lokaal misbruiken om zijn rechten te verhogen en SYSTEM-rechten te verkrijgen. Microsoft meldt dat de kwetsbaarheid actief wordt misbruikt. Er zijn geen details bekend over de wijze waarop de kwetsbaarheid bij aanvallen wordt misbruikt.

==**EINDE UPDATE**==

CVE-ID	CVSS	Component	Impact
CVE-2026-73025	9,80	iSCSI	Omzeilen van beveiligingsmaatregel

CVE-2026-69276	9,80	UxTheme Library	Uitvoeren van willekeurige code
CVE-2026-70296	9,80	Imaging	Uitvoeren van willekeurige code
CVE-2026-69730	9,80	DNS	Uitvoeren van willekeurige code
CVE-2026-69824	9,80	XPS	Uitvoeren van willekeurige code
CVE-2026-69590	9,80	RRAS	Uitvoeren van willekeurige code
CVE-2026-69463	9,80	NTFS	Uitvoeren van willekeurige code
CVE-2026-69669	9,80	NTFS	Uitvoeren van willekeurige code
CVE-2026-69845	9,80	DHCP Server	Uitvoeren van willekeurige code
CVE-2026-72979	9,80	DHCP Server	Uitvoeren van willekeurige code
CVE-2026-69595	9,80	NFS ONCRPC	Uitvoeren van willekeurige code
CVE-2026-78445	9,80	NFS ONCRPC	Uitvoeren van willekeurige code
CVE-2026-69829	9,80	SHELL	Uitvoeren van willekeurige code
CVE-2026-72983	9,80	ICS	Uitvoeren van willekeurige code
CVE-2026-69579	9,80	Message Queuing	Uitvoeren van willekeurige code
CVE-2026-69496	9,80	Compressed Folder	Uitvoeren van willekeurige code
CVE-2026-69774	9,00	Hyper-V	Uitvoeren van willekeurige code
CVE-2026-69910	9,80	Hyper-V	Uitvoeren van willekeurige code
CVE-2026-72982	9,80	Netlogon	Uitvoeren van willekeurige code
CVE-2026-69769	9,80	HTTP Print Provider	Uitvoeren van willekeurige code
CVE-2026-69431	9,80	Telnet Client	Uitvoeren van willekeurige code
CVE-2026-69639	9,80	Libarchive	Uitvoeren van willekeurige code

CVE-2026-69819	9,80	RPC Runtime	Uitvoeren van willekeurige code
CVE-2026-69493	9,80	Event Logging Service	Uitvoeren van willekeurige code
CVE-2026-69434	9,80	URL Moniker	Uitvoeren van willekeurige code
CVE-2026-69715	9,80	Direct Show	Uitvoeren van willekeurige code
CVE-2026-73009	9,80	SSTP	Uitvoeren van willekeurige code
CVE-2026-68839	9,80	USB Mass Storage Class	Uitvoeren van willekeurige code
CVE-2026-68839	9,80	Remote Desktop Services	Uitvoeren van willekeurige code
CVE-2026-69525	9,80	USB Mass Storage Class	Uitvoeren van willekeurige code
CVE-2026-73010	9,80	Failover Cluster	Uitvoeren van willekeurige code
CVE-2026-69768	9,80	RNDIS	Uitvoeren van willekeurige code
CVE-2026-77493	9,80	Office Outlook	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://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-68839	9.8 CRITICAL
CVE-2026-69276	9.8 CRITICAL
CVE-2026-69431	9.8 CRITICAL
CVE-2026-69434	8.8 HIGH
CVE-2026-69463	9.8 CRITICAL
CVE-2026-69493	9.8 CRITICAL
CVE-2026-69496	9.8 CRITICAL
CVE-2026-69525	9.8 CRITICAL
CVE-2026-69579	9.8 CRITICAL
CVE-2026-69590	9.8 CRITICAL
CVE-2026-69595	9.8 CRITICAL
CVE-2026-69639	
CVE-2026-69669	8.8 HIGH
CVE-2026-69715	9.8 CRITICAL
CVE-2026-69730	9.8 CRITICAL
CVE-2026-69768	9.8 CRITICAL
CVE-2026-69769	9.8 CRITICAL
CVE-2026-69774	
CVE-2026-69819	9.8 CRITICAL
CVE-2026-69824	9.8 CRITICAL
CVE-2026-69829	9.8 CRITICAL

CVE-2026-69845	9.8 CRITICAL
CVE-2026-69910	9.8 CRITICAL
CVE-2026-70296	9.8 CRITICAL
CVE-2026-72979	9.8 CRITICAL
CVE-2026-72982	9.8 CRITICAL
CVE-2026-72983	9.8 CRITICAL
CVE-2026-73009	9.8 CRITICAL
CVE-2026-73010	9.8 CRITICAL
CVE-2026-73025	9.8 CRITICAL
CVE-2026-77493	9.8 CRITICAL
CVE-2026-78445	9.8 CRITICAL
CVE-2026-81963	7.8 HIGH
CVE-2026-85880	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-191	Integer Underflow (Wrap or Wraparound)
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-415	Double Free
CWE-416	Use After Free

CWE-787	Out-of-bounds Write
CWE-1390	Weak Authentication
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-908	Use of Uninitialized Resource

Getroffen producten

Microsoft
Microsoft Windows 11 Version 26H1
Windows
Windows 10 1607
Windows 10 1809
Windows 10 21h2
Windows 10 22h2
Windows 10 Version 1607
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64- based Systems
Windows 10 Version 1809
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64- based Systems

Windows 10 Version 21H2
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
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 11 23H2
Windows 11 Version 23H2
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows 11 Version 24H2
Windows 11 Version 24H2 for ARM64-based Systems
Windows 11 Version 24H2 for x64-based Systems
Windows 11 Version 25H2 for ARM64-based Systems

Windows 11 Version 25H2 for x64-based Systems
Windows 11 Version 26H1 for ARM64-based Systems
Windows 11 version 26H1 for x64-based Systems
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

Disclaimer