Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0472

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Windows

Publicatiedatum: 10-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Microsoft heeft kwetsbaarheden verholpen in Windows.

Duiding

Een kwaadwillende kan de kwetsbaarheden mogelijk misbruiken om beveiligingsmaatregelen te omzeilen, privileges te verhogen, willekeurige code uit te voeren en/of toegang te verkrijgen tot gevoelige informatie.

De 13 ernstigste kwetsbaarheden bevinden zich in verschillende Windows-componenten en hebben een CVSS-score van 9,0 of hoger. Afhankelijk van de betreffende kwetsbaarheid kan misbruik leiden tot het uitvoeren van willekeurige code of het verkrijgen van verhoogde rechten.

De betreffende kwetsbaarheden zijn weergegeven in onderstaande tabel.

De overige kwetsbaarheden variëren in ernst van gemiddeld tot hoog. Het voert te ver om iedere kwetsbaarheid afzonderlijk in detail te behandelen in deze advisory. Raadpleeg het MSRC-portaal voor aanvullende informatie over de afzonderlijke kwetsbaarheden en de beschikbare beveiligingsupdates.

Windows iSCSI:

CVE-ID	CVSS	Impact
CVE-2026-88234	9.80	Uitvoeren van willekeurige code

Windows Virtual Filtering Platform (VFP):

CVE-ID	CVSS	Impact
CVE-2026-95962	9.00	Uitvoeren van willekeurige code

Windows DNS:

CVE-ID	CVSS	Impact
CVE-2026-88218	9.80	Uitvoeren van willekeurige code

Windows Xbox Live Networking Service:

CVE-ID	CVSS	Impact
CVE-2026-112967	9.80	Uitvoeren van willekeurige code

Microsoft Windows Media Foundation:

CVE-ID	CVSS	Impact

| CVE-2026-96157 | 9.80 | Uitvoeren van willekeurige code |

Windows DHCP Server:

CVE-ID	CVSS	Impact
CVE-2026-88243	9.80	Uitvoeren van willekeurige code

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2026-119958	9.80	Uitvoeren van willekeurige code

Microsoft Color Management:

CVE-ID	CVSS	Impact
CVE-2026-96067	9.80	Uitvoeren van willekeurige code
CVE-2026-96078	9.80	Uitvoeren van willekeurige code

Microsoft Exchange Server:

CVE-ID	CVSS	Impact
CVE-2026-116928	9.80	Uitvoeren van willekeurige code

Windows Kerberos:

CVE-ID	CVSS	Impact
CVE-2026-85844	9.80	Verkrijgen van verhoogde rechten

Windows Microsoft DirectMusic:

CVE-ID	CVSS	Impact
CVE-2026-95882	9.80	Uitvoeren van willekeurige code
CVE-2026-95901	9.80	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://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-85844	9.8 CRITICAL
CVE-2026-88218	9.8 CRITICAL
CVE-2026-88234	9.8 CRITICAL
CVE-2026-88243	9.8 CRITICAL
CVE-2026-95882	9.8 CRITICAL
CVE-2026-95901	9.8 CRITICAL
CVE-2026-95962	9.0 CRITICAL
CVE-2026-96067	9.8 CRITICAL
CVE-2026-96078	9.8 CRITICAL
CVE-2026-96157	9.8 CRITICAL
CVE-2026-112967	9.8 CRITICAL
CVE-2026-116928	9.8 CRITICAL
CVE-2026-119958	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal
CWE-59	Improper Link Resolution Before File Access
CWE-73	External Control of File Name or Path
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-94	Improper Control of Generation of Code
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-134	Use of Externally-Controlled Format String
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-193	Off-by-one Error
CWE-197	Numeric Truncation Error
CWE-283	Unverified Ownership
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-290	Authentication Bypass by Spoofing
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Functionality
CWE-326	Inadequate Encryption Strength
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-522	Insufficiently Protected Credentials

CWE	Beschrijving
CWE-552	Files or Directories Accessible to External Parties
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-763	Release of Invalid Pointer or Reference
CWE-787	Out-of-bounds Write
CWE-822	Untrusted Pointer Dereference
CWE-823	Use of Out-of-range Pointer Offset
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-843	Access of Resource Using Incompatible Type
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-908	Use of Uninitialized Resource
CWE-1037	Processor Optimization Removal or Modification of Security-critical Code
CWE-1220	Insufficient Granularity of Access Control
CWE-1390	Weak Authentication

Getroffen producten

Microsoft
Windows
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
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 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems

Microsoft
Windows 10 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
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 26H2 for ARM64-based Systems
Windows 11 Version 26H2 for x64-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
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2025
Windows Server 2025 (Server Core installation)

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.