



Advisory NCSC-2026-0423

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Windows

Publicatiedatum: 13-10-2026

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 delen. 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 1159 kwetsbaarheden verholpen in Windows.

Duiding

Het voert te ver om iedere kwetsbaarheid te benoemen. De 53 ernstigste kwetsbaarheden, met een CVSS score van 9 en hoger zijn weergegeven in onderstaande lijst en geven een kwaadwillende de mogelijkheid om zich voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen en willekeurige code uit te voeren. Deze kwetsbaarheden bevinden zich in diverse subcomponenten van Windows.

Voor daadwerkelijk misbruik hoeft geen voorafgaande authenticatie plaats te vinden en diverse kwetsbaarheden zijn op afstand, zonder gebruikersinteractie te misbruiken. Met name systemen die via publieke netwerken ontsloten zijn lopen hiermee verhoogd risico op misbruik.

|-----|---|-----|

CVE-ID	CVSS	Impact
CVE-2026-100202	9.80	Uitvoeren van willekeurige code
CVE-2026-100219	9.80	Uitvoeren van willekeurige code
CVE-2026-100222	9.80	Uitvoeren van willekeurige code
CVE-2026-102210	9.80	Uitvoeren van willekeurige code
CVE-2026-105008	9.00	Voordoen als andere gebruiker
CVE-2026-105010	9.80	Verkrijgen van verhoogde rechten
CVE-2026-105016	9.80	Uitvoeren van willekeurige code
CVE-2026-21413	9.80	Uitvoeren van willekeurige code
CVE-2026-69634	9.80	Uitvoeren van willekeurige code
CVE-2026-69639	9.80	Uitvoeren van willekeurige code
CVE-2026-69705	9.80	Uitvoeren van willekeurige code
CVE-2026-69883	9.80	Uitvoeren van willekeurige code
CVE-2026-69886	9.80	Uitvoeren van willekeurige code
CVE-2026-70024	9.80	Uitvoeren van willekeurige code
CVE-2026-70096	9.80	Uitvoeren van willekeurige code
CVE-2026-70147	9.80	Uitvoeren van willekeurige code
CVE-2026-70153	9.80	Uitvoeren van willekeurige code
CVE-2026-70157	9.80	Uitvoeren van willekeurige code
CVE-2026-70188	9.10	Omzeilen van beveiligingsmaatregel
CVE-2026-83517	9.80	Uitvoeren van willekeurige code
CVE-2026-83519	9.80	Uitvoeren van willekeurige code
CVE-2026-83578	9.80	Uitvoeren van willekeurige code
CVE-2026-83693	9.80	Uitvoeren van willekeurige code
CVE-2026-83748	9.80	Uitvoeren van willekeurige code
CVE-2026-83770	9.80	Uitvoeren van willekeurige code
CVE-2026-83780	9.80	Uitvoeren van willekeurige code
CVE-2026-83782	9.80	Uitvoeren van willekeurige code
CVE-2026-83862	9.80	Uitvoeren van willekeurige code
CVE-2026-83869	9.80	Uitvoeren van willekeurige code
CVE-2026-83910	9.80	Uitvoeren van willekeurige code
CVE-2026-83935	9.80	Uitvoeren van willekeurige code
CVE-2026-84015	9.80	Uitvoeren van willekeurige code
CVE-2026-85792	9.80	Uitvoeren van willekeurige code
CVE-2026-85806	9.80	Uitvoeren van willekeurige code
CVE-2026-85809	9.80	Uitvoeren van willekeurige code
CVE-2026-85814	9.80	Uitvoeren van willekeurige code
CVE-2026-85818	9.00	Voordoen als andere gebruiker
CVE-2026-85844	9.80	Verkrijgen van verhoogde rechten
CVE-2026-85928	9.80	Uitvoeren van willekeurige code
CVE-2026-88092	9.40	Manipulatie van gegevens
CVE-2026-88102	9.80	Uitvoeren van willekeurige code
CVE-2026-94510	9.90	Verkrijgen van verhoogde rechten
CVE-2026-96096	9.80	Uitvoeren van willekeurige code
CVE-2026-96219	9.80	Uitvoeren van willekeurige code
CVE-2026-96252	9.10	Voordoen als andere gebruiker
CVE-2026-96320	9.80	Uitvoeren van willekeurige code
CVE-2026-96864	9.80	Uitvoeren van willekeurige code
CVE-2026-96909	9.80	Uitvoeren van willekeurige code
CVE-2026-96924	9.80	Uitvoeren van willekeurige code
CVE-2026-96934	9.80	Uitvoeren van willekeurige code
CVE-2026-97814	9.80	Uitvoeren van willekeurige code
CVE-2026-97815	9.80	Uitvoeren van willekeurige code
CVE-2026-97816	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>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-100202	
CVE-2026-100219	
CVE-2026-100222	
CVE-2026-102210	
CVE-2026-105008	
CVE-2026-21413	9.8 CRITICAL
CVE-2026-69634	
CVE-2026-69639	
CVE-2026-69705	
CVE-2026-69883	
CVE-2026-69886	
CVE-2026-70024	
CVE-2026-70096	
CVE-2026-70147	
CVE-2026-70153	
CVE-2026-70157	
CVE-2026-70188	
CVE-2026-83517	
CVE-2026-83519	
CVE-2026-83578	
CVE-2026-83693	
CVE-2026-83748	

CVE	CVSS Score
CVE-2026-83770	
CVE-2026-83780	
CVE-2026-83782	
CVE-2026-83862	
CVE-2026-83869	
CVE-2026-83910	
CVE-2026-83935	
CVE-2026-84015	
CVE-2026-85792	
CVE-2026-85806	
CVE-2026-85809	
CVE-2026-85814	
CVE-2026-85818	
CVE-2026-85844	
CVE-2026-85928	
CVE-2026-88092	
CVE-2026-88102	
CVE-2026-94510	9.9 CRITICAL
CVE-2026-96096	
CVE-2026-96219	
CVE-2026-96252	
CVE-2026-96320	
CVE-2026-96864	
CVE-2026-96909	
CVE-2026-96924	
CVE-2026-96934	
CVE-2026-97814	
CVE-2026-97815	
CVE-2026-97816	
CVE-2026-105016	

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-129	Improper Validation of Array Index
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-347	Improper Verification of Cryptographic Signature
CWE-415	Double Free
CWE-416	Use After Free
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-787	Out-of-bounds Write
CWE-822	Untrusted Pointer Dereference

Getroffen producten

Microsoft
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
Windows 10 Version 22H2 for x64-based Systems

Microsoft

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 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 or 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.