



NCSC-2024-0470

Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-12-2024

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 aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Uitvoer van willekeurige code (Gebruikersrechten)
- Uitvoer van willekeurige code (Systeemrechten)
- Verkrijgen van verhoogde rechten
- Toegang tot gevoelige gegevens

De ernstigste kwetsbaarheid heeft kenmerk CVE-2024-49112 toegewezen gekregen en bevindt zich in de LDAP-component van de Domain Controller. Een kwaadwillende kan de kwetsbaarheid misbruiken om zonder voorafgaande authenticatie uitvoer van willekeurige code mogelijk te maken middels een malafide LDAP-call. Succesvol misbruik vereist wel dat de kwaadwillende LAN-toegang tot de Domain Controller heeft.

Windows Kernel-Mode Drivers:

CVE-ID	CVSS	Impact
CVE-2024-49074	7.80	Verkrijgen van verhoogde rechten

Remote Desktop Client:

CVE-ID	CVSS	Impact
CVE-2024-49105	8.40	Uitvoeren van willekeurige code

Windows Mobile Broadband:

CVE-ID	CVSS	Impact
CVE-2024-49073	6.80	Verkrijgen van verhoogde rechten
CVE-2024-49087	4.60	Toegang tot gevoelige gegevens
CVE-2024-49092	6.80	Verkrijgen van verhoogde rechten
CVE-2024-49077	6.80	Verkrijgen van verhoogde rechten

CVE-2024-49078	6.80	Verkrijgen van verhoogde rechten
CVE-2024-49083	6.80	Verkrijgen van verhoogde rechten
CVE-2024-49110	6.80	Verkrijgen van verhoogde rechten

Windows PrintWorkflowUserSvc:

CVE-ID	CVSS	Impact
CVE-2024-49097	7.00	Verkrijgen van verhoogde rechten
CVE-2024-49095	7.00	Verkrijgen van verhoogde rechten

Windows Kernel:

CVE-ID	CVSS	Impact
CVE-2024-49084	7.00	Verkrijgen van verhoogde rechten

Windows Remote Desktop:

CVE-ID	CVSS	Impact
CVE-2024-49132	8.10	Uitvoeren van willekeurige code

Windows Routing and Remote Access Service (RRAS):

CVE-ID	CVSS	Impact
CVE-2024-49085	8.80	Uitvoeren van willekeurige code
CVE-2024-49086	8.80	Uitvoeren van willekeurige code
CVE-2024-49089	7.20	Uitvoeren van willekeurige code
CVE-2024-49102	8.80	Uitvoeren van willekeurige code
CVE-2024-49104	8.80	Uitvoeren van willekeurige code
CVE-2024-49125	8.80	Uitvoeren van willekeurige code

Role: DNS Server:

CVE-ID	CVSS	Impact
--------	------	--------

CVE-ID	CVSS	Impact
CVE-2024-49091	7.20	Uitvoeren van willekeurige code

Role: Windows Hyper-V:

CVE-ID	CVSS	Impact
CVE-2024-49117	8.80	Uitvoeren van willekeurige code

Windows LDAP - Lightweight Directory Access Protocol:

CVE-ID	CVSS	Impact
CVE-2024-49121	7.50	Denial-of-Service
CVE-2024-49124	8.10	Uitvoeren van willekeurige code
CVE-2024-49112	9.80	Uitvoeren van willekeurige code
CVE-2024-49113	7.50	Denial-of-Service
CVE-2024-49127	8.10	Uitvoeren van willekeurige code

Microsoft Office Publisher:

CVE-ID	CVSS	Impact
CVE-2024-49079	7.80	Uitvoeren van willekeurige code

Windows IP Routing Management Snapin:

CVE-ID	CVSS	Impact
CVE-2024-49080	8.80	Uitvoeren van willekeurige code

Windows Resilient File System (ReFS):

CVE-ID	CVSS	Impact
--------	------	--------

CVE-2024-49093	8.80	Verkrijgen van verhoogde rechten
----------------	------	----------------------------------

Windows Task Scheduler:

CVE-ID	CVSS	Impact
CVE-2024-49072	7.80	Verkrijgen van verhoogde rechten

Windows Remote Desktop Services:

CVE-ID	CVSS	Impact
CVE-2024-49106	8.10	Uitvoeren van willekeurige code
CVE-2024-49108	8.10	Uitvoeren van willekeurige code
CVE-2024-49115	8.10	Uitvoeren van willekeurige code
CVE-2024-49119	8.10	Uitvoeren van willekeurige code
CVE-2024-49120	8.10	Uitvoeren van willekeurige code
CVE-2024-49123	8.10	Uitvoeren van willekeurige code
CVE-2024-49129	7.50	Denial-of-Service
CVE-2024-49075	7.50	Denial-of-Service
CVE-2024-49116	8.10	Uitvoeren van willekeurige code
CVE-2024-49128	8.10	Uitvoeren van willekeurige code

Windows Wireless Wide Area Network Service:

CVE-ID	CVSS	Impact
CVE-2024-49094	6.60	Verkrijgen van verhoogde rechten
CVE-2024-49098	4.30	Toegang tot gevoelige gegevens
CVE-2024-49099	4.30	Toegang tot gevoelige gegevens
CVE-2024-49101	6.60	Verkrijgen van verhoogde rechten
CVE-2024-49103	4.30	Toegang tot gevoelige gegevens
CVE-2024-49111	6.60	Verkrijgen van verhoogde rechten
CVE-2024-49081	6.60	Verkrijgen van verhoogde rechten
CVE-2024-49109	6.60	Verkrijgen van verhoogde rechten

WmsRepair Service:

CVE-ID	CVSS	Impact
CVE-2024-49107	7.30	Verkrijgen van verhoogde rechten

Windows Local Security Authority Subsystem Service (LSASS):

CVE-ID	CVSS	Impact
CVE-2024-49126	8.10	Uitvoeren van willekeurige code

Windows Message Queuing:

CVE-ID	CVSS	Impact
CVE-2024-49096	7.50	Denial-of-Service
CVE-2024-49122	8.10	Uitvoeren van willekeurige code
CVE-2024-49118	8.10	Uitvoeren van willekeurige code

Windows Common Log File System Driver:

CVE-ID	CVSS	Impact
CVE-2024-49088	7.80	Verkrijgen van verhoogde rechten
CVE-2024-49090	7.80	Verkrijgen van verhoogde rechten
CVE-2024-49138	7.80	Verkrijgen van verhoogde rechten

Windows Cloud Files Mini Filter Driver:

CVE-ID	CVSS	Impact
CVE-2024-49114	7.80	Verkrijgen van verhoogde rechten

Windows Virtualization-Based Security (VBS) Enclave:

CVE-ID	CVSS	Impact
--------	------	--------

-----	-----	-----
CVE-2024-49076	7.80	Verkrijgen van verhoogde rechten
-----	-----	-----

Windows File Explorer:

-----	-----	-----
CVE-ID	CVSS	Impact
-----	-----	-----
CVE-2024-49082	6.80	Toegang tot gevoelige gegevens
-----	-----	-----

System Center Operations Manager:

-----	-----	-----
CVE-ID	CVSS	Impact
-----	-----	-----
CVE-2024-43594	7.30	Verkrijgen van verhoogde rechten
-----	-----	-----

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-2024-49073	6.8 MEDIUM
> CVE-2024-49074	7.8 HIGH
> CVE-2024-49084	7.0 HIGH
> CVE-2024-49087	4.6 MEDIUM
> CVE-2024-49089	7.2 HIGH
> CVE-2024-49092	6.8 MEDIUM

> CVE-2024-49094	6.6 MEDIUM
> CVE-2024-49096	7.5 HIGH
> CVE-2024-49097	7.0 HIGH
> CVE-2024-49098	4.3 MEDIUM
> CVE-2024-49099	4.3 MEDIUM
> CVE-2024-49101	6.6 MEDIUM
> CVE-2024-49102	8.8 HIGH
> CVE-2024-49103	4.3 MEDIUM
> CVE-2024-49104	8.8 HIGH
> CVE-2024-49105	
> CVE-2024-49107	7.3 HIGH
> CVE-2024-49111	6.6 MEDIUM
> CVE-2024-49121	7.5 HIGH
> CVE-2024-49122	8.1 HIGH
> CVE-2024-49123	8.1 HIGH
> CVE-2024-49124	8.1 HIGH
> CVE-2024-49126	8.1 HIGH
> CVE-2024-49132	8.1 HIGH
> CVE-2024-49072	
> CVE-2024-49075	
> CVE-2024-49076	
> CVE-2024-49077	6.8 MEDIUM
> CVE-2024-49078	

> CVE-2024-49079	7.8 HIGH
> CVE-2024-49080	8.8 HIGH
> CVE-2024-49081	6.6 MEDIUM
> CVE-2024-49082	6.8 MEDIUM
> CVE-2024-49083	
> CVE-2024-49088	
> CVE-2024-49090	
> CVE-2024-49095	
> CVE-2024-49109	
> CVE-2024-49110	6.8 MEDIUM
> CVE-2024-49112	
> CVE-2024-49113	
> CVE-2024-49114	
> CVE-2024-49118	
> CVE-2024-49127	
> CVE-2024-49138	7.8 HIGH
> CVE-2024-49085	8.8 HIGH
> CVE-2024-49086	8.8 HIGH
> CVE-2024-49091	7.2 HIGH
> CVE-2024-49106	8.1 HIGH
> CVE-2024-49108	8.1 HIGH
> CVE-2024-49115	8.1 HIGH
> CVE-2024-49119	8.1 HIGH

> CVE-2024-49120	8.1 HIGH
> CVE-2024-49125	8.8 HIGH
> CVE-2024-49129	7.5 HIGH
> CVE-2024-49116	
> CVE-2024-49128	
> CVE-2024-49117	8.8 HIGH
> CVE-2024-49093	8.8 HIGH
> CVE-2024-43594	7.3 HIGH

CWE's

CWE	Beschrijving
> CVE-591	Sensitive Data Storage in Improperly Locked Memory
> CVE-393	Return of Wrong Status Code
> CVE-453	Insecure Default Variable Initialization
> CVE-820	Missing Synchronization
> CVE-59	Improper Link Resolution Before File Access ('Link Following')
> CVE-191	Integer Underflow (Wrap or Wraparound)
> CVE-822	Untrusted Pointer Dereference
> CVE-126	Buffer Over-read
> CVE-415	Double Free
> CVE-843	Access of Resource Using Incompatible Type ('Type Confusion')
> CVE-190	Integer Overflow or Wraparound
> CVE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CVE-125	Out-of-bounds Read

› CWE-284	Improper Access Control
› CWE-416	Use After Free
› CWE-476	NULL Pointer Dereference
› CWE-400	Uncontrolled Resource Consumption
› CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
› CWE-122	Heap-based Buffer Overflow
› CWE-681	Incorrect Conversion between Numeric Types
› CWE-20	Improper Input Validation
› CWE-287	Improper Authentication

Getroffen producten

microsoft
system_center_operations_manager
system_center_operations_manager__scom__2019
system_center_operations_manager__scom__2022
system_center_operations_manager__scom__2025
windows
windows_10_version_1507
windows_10_version_1607
windows_10_version_1809
windows_10_version_21h2
windows_10_version_22h2
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_
windows_server_2025
windows_server_2025__server_core_installation_
windows_10_1507
windows_10_1607
windows_10_1809
windows_10_21h2
windows_10_22h2
windows_11_22h2
windows_11_23h2
windows_11_24h2

windows_server_2008_r2
windows_server_2008_sp2
windows_server_23h2

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.