



Advisory NCSC-2026-0424

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Dynamics

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 kwetsbaarheden verholpen in diverse Dynamics componenten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade zoals benoemd in onderstaande tabellen:

Microsoft Dataverse: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-88131	9.80	Uitvoeren van willekeurige code

Dynamics Business Central: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-100214	8.80	Uitvoeren van willekeurige code
CVE-2026-102226	8.80	Verkrijgen van verhoogde rechten
CVE-2026-105727	8.80	Verkrijgen van verhoogde rechten
CVE-2026-105728	7.50	Toegang tot gevoelige gegevens

Microsoft Dynamics 365 (on-premises): |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-102848	8.10	Verkrijgen van verhoogde rechten

Microsoft Power Apps: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-70213	8.00	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-2026-102848	
CVE-2026-100214	
CVE-2026-102226	
CVE-2026-105727	
CVE-2026-70213	
CVE-2026-88131	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-346	Origin Validation Error
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Microsoft
Microsoft Dataverse
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Dynamics NAV 2017 on Windows Server 2012
Microsoft Dynamics NAV 2018 on Windows Server 2012

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.