



NCSC-2026-0392

Kwetsbaarheden verholpen in IBM Langflow OSS en IBM MQ Appliance

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-09-2026

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

IBM heeft 12 kwetsbaarheden verholpen in IBM MQ, IBM MQ Appliance en Langflow OSS.

Duiding

De kwetsbaarheden kunnen leiden tot het uitvoeren van willekeurige code of commando's. Vier kwetsbaarheden zijn als kritiek aangemerkt en kunnen zonder authenticatie en gebruikersinteractie op afstand worden misbruikt.

De kwetsbaarheid met kenmerk CVE-2026-10747 heeft een CVSS-score van 10,0 en betreft een heap-based buffer overflow in IBM MQ. De kwetsbaarheden met kenmerk CVE-2026-79724, CVE-2026-85025 en CVE-2026-81204 hebben een CVSS-score van 9,8 en bevinden zich in Langflow OSS. Een niet-geauthenticeerde kwaadwillende kan deze kwetsbaarheden misbruiken om willekeurige code of OS-commando's uit te voeren. De overige kwetsbaarheden in Langflow hebben een CVSS-score van 8,8 en vereisen geauthenticeerde toegang.

Oplossingen

IBM heeft updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.ibm.com/support/pages/node/7284543>
- <https://www.ibm.com/support/pages/node/7286666>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-76059	8.8 HIGH
➤ CVE-2026-78569	8.8 HIGH
➤ CVE-2026-78571	8.8 HIGH
➤ CVE-2026-78575	8.8 HIGH
➤ CVE-2026-79724	9.8 CRITICAL
➤ CVE-2026-79742	8.8 HIGH

> CVE-2026-81204	9.8 CRITICAL
> CVE-2026-81211	8.8 HIGH
> CVE-2026-81940	8.8 HIGH
> CVE-2026-81941	8.8 HIGH
> CVE-2026-85025	9.8 CRITICAL

CWE's

CWE	Beschrijving
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-862	Missing Authorization
> CWE-863	Incorrect Authorization

Getroffen producten

IBM
IBM MQ Appliance
Langflow OSS

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.