Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0251

Kwetsbaarheden verholpen in IBM Langflow OSS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-07-2026

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 meerdere kwetsbaarheden verholpen in IBM Langflow OSS versies 1.0.0 tot en met 1.10.0.

Duiding

De kwetsbaarheden in IBM Langflow OSS betreffen onder andere:

- het uitvoeren van willekeurige bestandswijzigingen door geauthenticeerde gebruikers via speciaal opgemaakte Content-Disposition headers
- server-side request forgery (SSRF) door onveilige standaardconfiguraties
- remote code execution (RCE) door onvoldoende validatie van MCP serverconfiguratiebestanden
- geauthenticeerde gebruikers kunnen bestanden lezen, waaronder de JWT signing key, wat het mogelijk maakt authenticatietokens te vervalsen
- een kwetsbaarheid in de apply_tweaks() functie die parameteroverriding via de API toestaat en unsafe deserialisatie in de AsyncDiskCache class die RCE mogelijk maakt
- het POST /api/v1/validate/code endpoint voert gebruikersgeleverde Python code uit zonder sandboxing, wat volledige servercontrole kan geven
- de webhook authenticatiemechanismen kunnen worden omzeild als de WEBHOOK_AUTH_ENABLE parameter op False staat, waardoor ongeauthenticeerde gebruikers flows kunnen uitvoeren
- ook is er een privilege escalation mogelijk tot superuser via het misbruiken van Langflow service permissies
- een path traversal kwetsbaarheid in de APIRequest component maakt het mogelijk om bestanden op ongewenste locaties te schrijven
- het /api/v1/login/auto_login endpoint kan bij ingeschakelde AUTO_LOGIN feature langelevensduur superuser tokens uitgeven zonder authenticatie, mede verergerd door permissieve CORS instellingen
- de Policies component bevat een code injection kwetsbaarheid in de ToolGuard integratie, waarbij geauthenticeerde gebruikers met flow creatie rechten arbitrary Python code kunnen uitvoeren
- ongeauthenticeerde aanvallers kunnen superuser tokens verkrijgen en daarmee volledige remote code execution uitvoeren op standaardinstallaties. Tevens kunnen zij een onbeperkt aantal actieve gebruikersaccounts aanmaken als de NEW_USER_IS_ACTIVE parameter op true staat, waarmee ze de AUTO_LOGIN restricties kunnen omzeilen en toegang krijgen tot remote code execution endpoints.

Oplossingen

IBM heeft updates uitgebracht om de kwetsbaarheden in IBM Langflow OSS te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.ibm.com/support/pages/node/7278920
- https://www.ibm.com/support/pages/node/7278921
- https://www.ibm.com/support/pages/node/7278922
- https://www.ibm.com/support/pages/node/7278923
- https://www.ibm.com/support/pages/node/7278924
- https://www.ibm.com/support/pages/node/7278925
- https://www.ibm.com/support/pages/node/7278926
- https://www.ibm.com/support/pages/node/7278927
- https://www.ibm.com/support/pages/node/7278929
- https://www.ibm.com/support/pages/node/7278930
- https://www.ibm.com/support/pages/node/7278931
- https://www.ibm.com/support/pages/node/7278932
- https://www.ibm.com/support/pages/node/7278933
- https://www.ibm.com/support/pages/node/7278934
- https://www.ibm.com/support/pages/node/7279987
- https://www.ibm.com/support/pages/node/7279988
- https://www.ibm.com/support/pages/node/7279989
- https://www.ibm.com/support/pages/node/7279990
- https://www.ibm.com/support/pages/node/7279991
- https://www.ibm.com/support/pages/node/7279993
- https://www.ibm.com/support/pages/node/7279994
- https://www.ibm.com/support/pages/node/7279995
- https://www.ibm.com/support/pages/node/7279996
- https://www.ibm.com/support/pages/node/7279997

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-7667	5.3 MEDIUM
CVE-2026-7754	6.9 MEDIUM
CVE-2026-7755	10.0 CRITICAL
CVE-2026-7872	5.3 MEDIUM
CVE-2026-8056	5.3 MEDIUM

CVE-2026-8476	6.9 MEDIUM
CVE-2026-8481	5.3 MEDIUM
CVE-2026-8505	6.9 MEDIUM
CVE-2026-8635	9.4 CRITICAL
CVE-2026-8859	6.9 MEDIUM
CVE-2026-9103	9.8 CRITICAL
CVE-2026-9135	9.9 CRITICAL
CVE-2026-9198	9.8 CRITICAL
CVE-2026-9202	9.8 CRITICAL
CVE-2026-14499	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-265	Privilege Issues
CWE-275	Permission Issues
CWE-287	Improper Authentication
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

IBM
Langflow
Langflow Desktop
Langflow OSS

Disclaimer