National Cyber Security Centre

2409090130-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple vulnerabilities in IBM webMethods Integration

Monday 9th September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-09-04T16:15:00
Vendor: IBM
Product: webMethods Integration;
CVE ID: CVE-2024-45076
CVSS3.x Score[1]**:** 9.9
EPSS[2]**:** 0.199700000
(For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-45076)

Summary: IBM webMethods Integration 10.15 could allow an authenticated user to upload and execute arbitrary files which could be executed on the underlying operating system.

Published: 2024-09-04T16:15:00
Vendor: IBM
Product: webMethods Integration;
CVE ID: CVE-2024-45075
CVSS3.x Score: 8.8
EPSS: 0.199700000

Summary: IBM webMethods Integration 10.15 could allow an authenticated user to create scheduler tasks that would allow them to escalate their privileges to administrator due to missing authentication.

Published: 2024-09-04T16:15:00
Vendor: IBM
Product: webMethods Integration;
CVE ID: CVE-2024-45074
CVSS3.x Score: 6.5
EPSS: 0.197250000

Summary: IBM webMethods Integration 10.15 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.

Products Affected

- IBM webMethods Integration 10.15

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

Impact

Common Weakness Enumeration (CWE)[3]:

- CWE-434: Unrestricted Upload of File with Dangerous Type,
- CWE-308: Use of Single-factor Authentication,
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory (’Path Traversal’)

Present in CISA Known Exploited Vulnerability(KEV)[4] catalog: NO
Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from IBM.

Additional recommendations and mitigation’s for CVE-2024-45076, CVE-2024-45075 and CVE-2024-45074 can be found in the respective links below:

https://exchange.xforce.ibmcloud.com/vulnerabilities/351740;
https://exchange.xforce.ibmcloud.com/vulnerabilities/351738;
https://exchange.xforce.ibmcloud.com/vulnerabilities/351729;

[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre