XML External Entity Injection via Publisher in WSO2 API Manager Allows Reading Arbitrary Files

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-8010
State	PUBLISHED
Assigner	WSO2
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 10:16:14 UTC
Updated	2026-04-23 15:35:27 UTC
Description	The component accepts XML input through the publisher without disabling external entity resolution. This allows malicious a

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.000040000 probability, percentile 0.001840000 (date 2026-04-21)

Problem Types: CWE-611 | CWE-611 CWE-611: Improper Restriction of XML External Entity Reference ('XXE')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	ed10eef1-636d-4fbe-9993-6890dfa878f8	Secondary	3.5	LOW	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	3.5	LOW	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wso2	Api Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WSO2	WSO2 API Manager	unknown 3.2.0 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.0 3.2.0.397 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.1 3.2.1.27 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.0.0 4.0.0.310 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.0.0 4.0.0.319 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.1.0 4.1.0.171 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.2.0 4.2.0.127 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.3.0 4.3.0.39 custom	Not specified

References

Reference	Source	Link
security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO...	ed10eef1-636d-4fbe-9993-6890dfa878f8	secu
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Follow the instructions given on https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2024-3581/#solution

There are currently no legacy CID mappings associated with this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**