XML External Entity Injection in Multiple WSO2 Products Allows Arbitrary file read and Denial of Service

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

Summary

CVE	CVE-2024-2374
State	PUBLISHED
Assigner	WSO2
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 09:16:34 UTC
Updated	2026-04-23 15:36:05 UTC
Description	The XML parsers within multiple WSO2 products accept user-supplied XML data without properly configuring to prevent the

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from nvd@nist.gov

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

EPSS: 0.000110000 probability, percentile 0.012950000 (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	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	ed10eef1-636d-4fbe-9993-6890dfa878f8	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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

High

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

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 3.1.0 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.1.0 3.1.0.278 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.0 3.2.0.368 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.0.0 4.0.0.280 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.1.0 4.1.0.206 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.2.0 4.2.0.144 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.3.0 4.3.0.57 custom	Not specified
CNA	WSO2	WSO2 Identity Server	unknown 5.10.0 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.10.0 5.10.0.300 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.11.0 5.11.0.329 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 6.0.0 6.0.0.179 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 6.1.0 6.1.0.136 custom	Not specified
CNA	WSO2	WSO2 Open Banking AM	unknown 2.0.0 custom	Not specified
CNA	WSO2	WSO2 Open Banking AM	affected 2.0.0 2.0.0.328 custom	Not specified
CNA	WSO2	WSO2 Open Banking IAM	unknown 2.0.0 custom	Not specified
CNA	WSO2	WSO2 Open Banking IAM	affected 2.0.0 2.0.0.348 custom	Not specified
CNA	WSO2	WSO2 Identity Server As Key Manager	unknown 5.10.0 custom	Not specified
CNA	WSO2	WSO2 Identity Server As Key Manager	affected 5.10.0 5.10.0.296 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/WSO2-2024-3255/#solution

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