Cross-Site Scripting via Authentication Endpoint in Multiple WSO2 Products Allows Redirection to Malicious Websites

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

Summary

CVE	CVE-2025-6024
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 15:35:04 UTC
Description	The authentication endpoint fails to encode user-supplied input before rendering it in the web page, allowing for script inject

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from ed10eef1-636d-4fbe-9993-6890dfa878f8

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

EPSS: 0.000110000 probability, percentile 0.013930000 (date 2026-04-26)

Problem Types: CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	ed10eef1-636d-4fbe-9993-6890dfa878f8	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wso2	Api Manager	3.1.0	All	All	All
Application	Wso2	Api Manager	3.2.0	All	All	All
Application	Wso2	Api Manager	3.2.1	All	All	All
Application	Wso2	Api Manager	4.0.0	All	All	All
Application	Wso2	Api Manager	4.1.0	-	All	All
Application	Wso2	Identity Server	5.10.0	All	All	All
Application	Wso2	Identity Server	5.11.0	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 3.1.0.351 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.0 3.2.0.455 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.1 3.2.1.74 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.0.0 4.0.0.375 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.1.0 4.1.0.238 custom	Not specified
CNA	WSO2	WSO2 Identity Server	unknown 5.10.0 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.10.0 5.10.0.360 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.11.0 5.11.0.405 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/WSO2-2025-4251/#solution

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