Improper Access Control via Gateway API in Multiple WSO2 Products Allows Unauthorized Operations

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

Summary

CVE	CVE-2025-8325
State	PUBLISHED
Assigner	WSO2
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 10:16:13 UTC
Updated	2026-05-11 10:16:13 UTC
Description	The software fails to enforce role-based access controls for certain Gateway API invocations. Users with the 'Internal/Every

Risk And Classification

Primary CVSS: v3.1 6.3 MEDIUM from ed10eef1-636d-4fbe-9993-6890dfa878f8

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

EPSS: 0.000340000 probability, percentile 0.100180000 (date 2026-05-12)

Problem Types: CWE-281 | CWE-281 CWE-281: Assigning Permissions Instead of Checking Them

Version	Source	Type	Score	Severity	Vector
3.1	ed10eef1-636d-4fbe-9993-6890dfa878f8	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WSO2	WSO2 API Control Plane	affected 4.5.0 4.5.0.18 custom	Not specified
CNA	WSO2	WSO2 Universal Gateway	affected 4.5.0 4.5.0.17 custom	Not specified
CNA	WSO2	WSO2 Traffic Manager	affected 4.5.0 4.5.0.17 custom	Not specified
CNA	WSO2	WSO2 API Manager	unknown 3.2.0 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.0 3.2.0.435 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 3.2.1 3.2.1.55 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.0.0 4.0.0.355 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.1.0 4.1.0.219 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.2.0 4.2.0.157 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.3.0 4.3.0.70 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.4.0 4.4.0.33 custom	Not specified
CNA	WSO2	WSO2 API Manager	affected 4.5.0 4.5.0.17 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 6.7.206 6.7.206.563 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 6.7.210 6.7.210.55 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.0.174 9.0.174.513 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.20.74 9.20.74.375 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.28.116 9.28.116.352 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.29.120 9.29.120.177 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.30.67 9.30.67.100 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	affected 9.31.86 9.31.86.58 custom	Not specified
CNA	WSO2	WSO2 Carbon API Management Implementation	unaffected 9.32.75 * custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 6.7.206 6.7.206.563 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 6.7.210 6.7.210.55 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.0.174 9.0.174.513 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.20.74 9.20.74.375 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.28.116 9.28.116.352 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.29.120 9.29.120.177 custom	Not specified

CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.30.67 9.30.67.100 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	affected 9.31.86 9.31.86.58 custom	Not specified
CNA	WSO2	WSO2 Carbon API Manager Rest API Utility	unaffected 9.32.75 * 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/WSO2-2025-4401/#solution

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