



Username Enumeration via Email OTP Flow in Multiple WSO2 Products Allows User Account Discovery

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-0391
State	PUBLISHED
Assigner	WSO2
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 10:16:11 UTC
Updated	2026-05-11 10:16:11 UTC
Description	The check user account lock states feature within the email OTP flow fails to validate user input, allowing an attacker to infe

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ed10eef1-636d-4fbe-9993-6890dfa878f8

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

EPSS: 0.000230000 probability, percentile 0.066000000 (date 2026-05-12)

Problem Types: CWE-204 | CWE-204 CWE-204 Observable response discrepancy

Version	Source	Type	Score	Severity	Vector
3.1	ed10eef1-636d-4fbe-9993-6890dfa878f8	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/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

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WSO2	WSO2 Identity Server	unknown 5.10.0 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.10.0 5.10.0.379 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.11.0 5.11.0.426 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 5.11.0 5.11.0.431 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 6.0.0 6.0.0.253 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 6.1.0 6.1.0.254 custom	Not specified
CNA	WSO2	WSO2 Identity Server	affected 7.0.0 7.0.0.131 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 2.0.0.318 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 5.10.0.267 custom	Not specified
CNA	WSO2	Email OTP Authenticator	affected 1.0.18 1.0.18.7 custom	Not specified
CNA	WSO2	Email OTP Authenticator	unaffected 1.0.24 * custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	affected 4.1.0 4.1.0.8 custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	affected 4.1.4 4.1.4.9 custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	unaffected 4.1.22 * custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	affected 3.0.5 3.0.5.8 custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	affected 3.0.24 3.0.24.6 custom	Not specified
CNA	WSO2	WSO2 Carbon Authenticator Library For EmailOTP	affected 3.0.26 3.0.26.16 custom	Not specified

References

Reference	Source	Link
security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO...	ed10eef1-636d-4f8e-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/WSO2-2024-3115/#solution>

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 registered 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