



WordPress Zoho Flow Plugin <= 2.14.1 - Cross Site Request Forgery (CSRF) Vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2025-59568
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-22 19:16:24 UTC
Updated	2026-04-23 15:34:04 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Flow Zoho Flow zoho-flow allows Cross Site Request Forgery. This

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.000130000 probability, percentile 0.021080000 (date 2026-04-23)

Problem Types: CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zoho Flow	Zoho Flow	affected 2.14.1 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/zoho-flow/vulnerability/wordpress-z...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

Vendor Comments And Credit

Discovery Credit

CNA: Bao - BlueRock | Patchstack Bug Bounty Program (en)

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