



InstaWP Connect <= 0.0.9.18 - Missing Authorization to Unauthenticated Post/Taxonomy/User Add/Change/Delete, Customizer Setting Change, Plugin Installation/Activation/Deactivation via events_receiver

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

Summary

CVE	CVE-2023-3956
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-27 07:15:09 UTC
Updated	2026-04-08 18:18:11 UTC
Description	The InstaWP Connect plugin for WordPress is vulnerable to unauthorized access of data, modification of data and loss of d

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Instawp	Instawp Connect	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Instawp	InstaWP Connect 1-click WP Staging Migration	affected 0.0.9.18 semver	Not specified

References

Reference

- InstaWP Connect <= 0.0.9.18 - Missing Authorization to Unauthenticated Post/Taxonomy/User Add/Change/Delete, Customizer Setting Change
- 403 Forbidden
- 403 Forbidden
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-07-22T00:00:00.000Z	Discovered
CNA	2023-07-22T00:00:00.000Z	Vendor Notified
CNA	2023-07-26T00:00:00.000Z	Disclosed

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](#)