



MStore API <= 4.10.7 - Unauthorized Account Access and Privilege Escalation

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

Summary

CVE	CVE-2023-3277
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 12:15:08 UTC
Updated	2026-04-08 17:16:59 UTC
Description	The MStore API plugin for WordPress is vulnerable to Unauthorized Account Access and Privilege Escalation in versions up to 4.10.7. An attacker with access to the MStore API can bypass authentication and escalate their privileges to administrator.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

Problem Types: CWE-288 | NVD-CWE-Other | CWE-288 CWE-288 Authentication Bypass Using an Alternate Path or Channel

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
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

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	Inspireui	Mstore Api	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Inspireui	MStore API Create Native Android IOS Apps On The Cloud	affected 4.10.7 semver	Not specified

References

Reference	Source	Link
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
MStore API <= 4.10.7 - Unauthorized Account Access and Privilege Escalation	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Truoc Phan (en)

CNA: An Đăng (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-06-19T00:00:00.000Z	Disclosed

Legacy QID Mappings

731040 WordPress Plugin Mstore-api Unauthenticated Privilege Escalation Vulnerability

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