



Sp*tify Play Button for WordPress <= 2.07 - Authenticated (Administrator+) Stored Cross-Site Scripting

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2023-1840
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-04 20:15:07 UTC
Updated	2026-04-08 17:16:53 UTC
Description	The Sp*tify Play Button for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	High
User Interaction	Required
Scope	Changed

Confidentiality

Low

Integrity

Low

Availability

None

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



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Followmedarling	Spotify-play-button-for-wordpress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jonkastonka	Sp*tify Play Button For WordPress	affected 2.07 semver	Not specified

References

Reference	Source
403 Forbidden	af854a3a-2127-422b-91ae-364da26
Sp*tify Play Button for WordPress <= 2.07 - Authenticated (Administrator+) Stored Cross-Site Scripting	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



Vendor Comments And Credit

Discovery Credit
CNA: Marco Wotschka (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-03-29T00:00:00.000Z	Discovered
CNA	2023-04-03T00:00:00.000Z	Vendor Notified
CNA	2023-04-04T00:00:00.000Z	Disclosed

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

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