



ContentStudio <= 1.2.5 - Authorization Bypass

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

Summary

CVE	CVE-2023-0558
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-27 22:15:09 UTC
Updated	2026-04-08 19:18:01 UTC
Description	The ContentStudio plugin for WordPress is vulnerable to authorization bypass due to an unsecure token check that is suscep

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](#)

EPSS: 0.015680000 probability, percentile 0.815090000 (date 2026-04-08)

Problem Types: CWE-639 | NVD-CWE-noinfo | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

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	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
3.1	CNA	DECLARED	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

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	Contentstudio	Contentstudio	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Contentstudio	ContentStudio	affected 1.2.5 semver	Not specified

References

Reference	Source	Link	Tags
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org	Exploit, Release N
ContentStudio <= 1.2.5 - Authorization Bypass	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.com	Third Party Adviso
Login Wordfence Threat Intelligence	MITRE	ti.wordfence.io	
ContentStudio <= 1.2.5 - Authorization Bypass	MITRE	www.wordfence.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

Vendor Comments And Credit

Discovery Credit

CNA: Chloe Chamberland (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-01-06T00:00:00.000Z	Discovered
CNA	2023-01-27T00:00:00.000Z	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