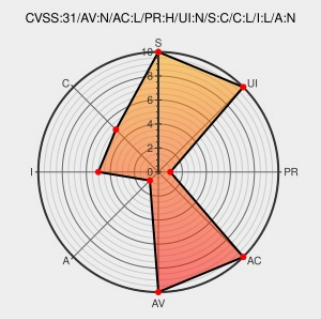
CVE-2021-39356

Published on: 10/21/2021 12:00:00 AM UTC

Last Modified on: 10/27/2021 10:25:00 PM UTC

CVE-2021-39356

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Content Staging from Content Staging Project contain the following vulnerability:

The Content Staging WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via several parameters that are echo'd out via the ~/templates/settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.

CVE-2021-39356 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Content Staging** - **Content Staging** version **<= 2.0.1**

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
word-press/Content Staging.md at main · BigTiger2020/word-press · GitHub	github.com text/html	MISC github.com/BigTiger2020/word-press/blob/main/Content%20Staging.md
Vulnerability Advisories - Wordfence	wordfence.com text/html	MISC wordfence.com/vulnerability-advisories/#CVE-2021-39356
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/content-staging/trunk/templates/settings.php

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Content Staging Project	Content Staging	All	All	All	All

cpe:2.3:a:content_staging_project:content_staging:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Thinkland Security Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39356 : The Content Staging WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insuffici… twitter.com/i/web/status/1…	2021-10-21 20:06:32
@LinInfoSec	Wordpress - CVE-2021-39356: wordfence.com/vulnerability-…	2021-10-28 00:21:37

← Previous ID

Next ID→