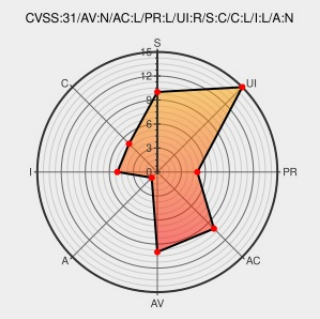
CVE-2020-35581

Published on: 01/15/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:47 PM UTC

CVE-2020-35581

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



Certain versions of Envira Gallery from Enviragallery contain the following vulnerability:

A stored cross-site scripting (XSS) issue in Envira Gallery Lite before 1.8.3.3 allows remote attackers to inject arbitrary JavaScript/HTML code via a POST /wp-admin/admin-ajax.php request with the meta[title] parameter.

CVE-2020-35581 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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
Envira Gallery Lite 1.8.3.2 Cross Site Scripting ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160924/Envira-Gallery-Lite-1.8.3.2-Cross-Site-Scripting.html

1.8.3.3 bump version, changelog · enviragallery/envira-gallery-lite@1026515 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/enviragallery/envira-gallery-lite/commit/102651514e6faca914ec1c7e113def340d8e1e09
escape title output · enviragallery/envira-gallery-lite@3b081dd · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/enviragallery/envira-gallery-lite/commit/3b081dd10a1731f8cd981bebeac0e775fb217acf
envira-gallery-lite/changelog.txt at master · enviragallery/envira-gallery-lite · GitHub	Release Notes Third Party Advisory github.com text/html	CONFIRM github.com/enviragallery/envira-gallery-lite/blob/master/changelog.txt

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Enviragallery	Envira Gallery	All	All	All	All
Application	Enviragallery	Envira Gallery	All	All	All	All

cpe:2.3:a:enviragallery:envira_gallery:*:*:*:*:lite:wordpress:*:*:

cpe:2.3:a:enviragallery:envira_gallery:*:*:*:*:lite:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→