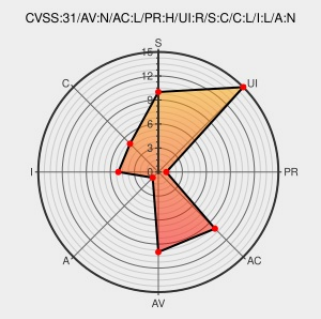
CVE-2022-3753

Published on: Not Yet Published

Last Modified on: 11/29/2022 02:09:05 PM UTC

CVE-2022-3753

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



Certain versions of Evaluate from Evaluate Project contain the following vulnerability:

The Evaluate WordPress plugin through 1.0 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).

CVE-2022-3753 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Unknown** - **Evaluate** version **= 0**

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

CVE References

Description	Tags	Link
Evaluate <= 1.0 - Admin+ Stored Cross-Site Scripting WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	CONFIRM wpscan.com/vulnerability/8e88a5b9-6f1d-40de-99fc-8e1e66646c2b

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Evaluate Project	Evaluate	All	All	All	All

cpe:2.3:a:evaluate_project:evaluate:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3753 : The Evaluate WordPress plugin through 1.0 does not sanitize and escapes some of its settings, which… twitter.com/i/web/status/1…	2022-11-21 11:08:31
/r/netcve	CVE-2022-3753	2022-11-21 12:38:42

← Previous ID

Next ID→