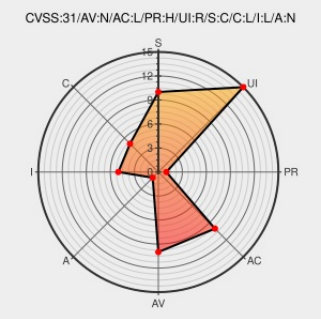
CVE-2022-3220

Published on: Not Yet Published

Last Modified on: 10/12/2022 04:47:00 PM UTC

CVE-2022-3220

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



Certain versions of Advanced Comment Form from Webgilde contain the following vulnerability:

The Advanced Comment Form WordPress plugin before 1.2.1 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.

CVE-2022-3220 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Unknown** - **Advanced Comment Form** version **< 1.2.1**

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

CVE References

Description	Tags	Link
Advanced Comment Form < 1.2.1 - Admin+ Authenticated Stored XSS WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/cb6f4953-e68b-48f3-a821-a1d77e5476ef

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webgilde	Advanced Comment Form	All	All	All	All

cpe:2.3:a:webgilde:advanced_comment_form:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Asif Nawaz Minhas

Social Mentions

Source	Title	Posted (UTC)
@hogehuga	curlで複数の脆弱性が公開された。 - CVE-2022-3220(5678) - seclists.org/oss-sec/2022/q… - 212 - (Set-Cookie|HTTP compression) denial of… twitter.com/i/web/status/1…	2022-06-27 06:53:16
@CVEreport	CVE-2022-3220 : The Advanced Comment Form WordPress plugin before 1.2.1 does not sanitise and escape its settings,… twitter.com/i/web/status/1…	2022-10-10 20:53:10
/r/netcve	CVE-2022-3220	2022-10-10 21:39:00

← Previous ID

Next ID→