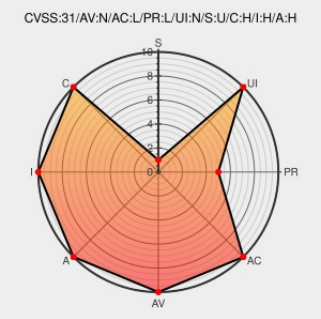
CVE-2022-1683

Published on: Not Yet Published

Last Modified on: 06/15/2022 04:12:00 PM UTC

CVE-2022-1683

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



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

The amtyThumb WordPress plugin through 4.2.0 does not sanitise and escape a parameter before using it in a SQL statement via its shortcode, leading to an SQL injection and is exploitable by any authenticated user (and not just Author+ like the original advisory mention) due to the fact that they can execute shortcodes via an AJAX action

CVE-2022-1683 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Unknown** - **amtyThumb** version **<= 4.2.0**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/359d145b-c365-4e7c-a12e-c26b7b8617ce
Security Bulletin	bulletin.iese.de text/html	MISC bulletin.iese.de/post/amtythumb_4-2-0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:amtythumb_project:amtythumb:*:*:*:*:*:wordpress:*:*

Discovery Credit

Daniel Krohmer (Fraunhofer IESE)

Shi Chen (University of Kaiserslautern)

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-1683 The amtyThumb WordPress plugin through 4.2.0 does not sanitise and… twitter.com/i/web/status/1…	2022-06-06 09:56:01
@CVEreport	CVE-2022-1683 : The amtyThumb WordPress plugin through 4.2.0 does not sanitise and escape a parameter before using… twitter.com/i/web/status/1…	2022-06-08 10:14:55
@LinInfoSec	Wordpress - CVE-2022-1683: wpscan.com/vulnerability/…	2022-06-08 13:01:07
@phpadvisories	CVE-2022-1683 | amtyThumb Plugin bis 4.2.0 auf WordPress Shortcode a SQL Injection zpr.io/iQb5Y3XRmUHs #phpsec	2022-06-08 16:16:23
/r/netcve	CVE-2022-1683	2022-06-08 10:38:56

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report