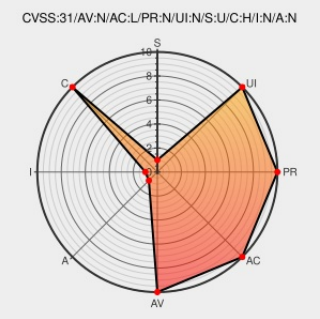
CVE-2015-20067

Published on: 11/01/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:16 PM UTC

CVE-2015-20067

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



Certain versions of Wp Attachment Export from Wp Attachment Export Project contain the following vulnerability:

The WP Attachment Export WordPress plugin before 0.2.4 does not have proper access controls, allowing unauthenticated users to download the XML data that holds all the details of attachments/posts on a Wordpress

CVE-2015-20067 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Unknown** - **WP Attachment Export** version **< 0.2.4**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Full Disclosure: Arbitrary File Download in WP Attachment Export Wordpress Plugin v0.2.3	seclists.org text/html	MISC seclists.org/fulldisclosure/2015/Jul/73

wpsploit/wp_attachment_export_file_download.rb at master · espreto/wpsploit · GitHub	github.com text/html	MISC github.com/espreto/wpsploit/blob/master/modules/auxiliary/sc
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/d1a9ed65-baf3-4c85-b077

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	Wp Attachment Export Project	Wp Attachment Export	All	All	All	All

cpe:2.3:a:wp_attachment_export_project:wp_attachment_export:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Nitin Venkatesh

← Previous ID

Next ID→