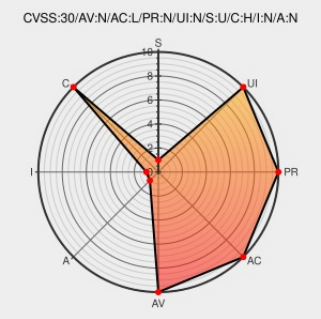
CVE-2018-7204

Published on: 03/07/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7204

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



Certain versions of File Manager from Giribaz contain the following vulnerability:

inc/logger.php in the Giribaz File Manager plugin before 5.0.2 for WordPress logged activity related to the plugin in /wp-content/uploads/file-manager/log.txt. If a user edits the wp-config.php file using this plugin, the wp-config.php contents get added to log.txt, which is not protected and contains database credentials, salts, etc. These files have been indexed by Google and a simple dork will find affected sites.

CVE-2018-7204 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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
File Manager <= 5.0.0 - Information Disclosure	Third Party Advisory web.archive.org	MISC wpvulndb.com/vulnerabilities/9036

	text/html Inactive Link Not Archived	
Changeset 1823035 for file-manager – WordPress Plugin Repository	Patch Third Party Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM plugins.trac.wordpress.org/changeset/1823035/file-manager
File Manager | WordPress.org	Third Party Advisory wordpress.org text/html	CONFIRM wordpress.org/plugins/file-manager/#developers

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	Giribaz	File Manager	All	All	All	All

cpe:2.3:a:giribaz:file_manager:*:*:*:*:*:wordpress:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→