Possible upload of PHAR files and wrong check of backslash in filenames

Moderate **Fasse** published **GHSA-xpqj-67r8-25j2** on May 20, 2021

Package

No package listed

Affected versions

4.0.3

Patched versions

4.0.4

Description

Impact

-Authenticated RCE via .PHAR File Upload. Need admin or upload permissions.
A php web shell can be uploaded via the Documents & Files upload feature. Someone with upload permissions could rename the php shell with a .phar extension, visit the file, triggering the payload for a reverse/bind shell. This can be mitigated by excluding a .phar file extension to be uploaded (like you did with .php .phtml .php5 etc)

-Authenticated Local File Inclusion. Need admin or upload permissions.
Someone with upload permissions can use the move to db ability to "get" local files and move to the Documents & Folders view. The mitigation to block "/" from file names works, but if you double encode it, it bypasses the check...

http://127.0.0.1/admidio/adm_program/modules/documents-files/documents_files_function.php?mode=6&folder_id=1&name=%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252fetc%252fpasswd

This example should load /etc/passwd to the files and docs page for someone to download and read. This might be able to be mitigated by using a strip slashes type of function in php before the function is called. (I think line 341-342 in documents_files_function.php)

-Unauthenticated Information Disclosure via exposed MySQL backups.
This is mostly a default apache config that could be considered a "misconfiguration" by users who install Admidio. If indexing in apache is allowed (it is be default), and an admin creates a db backup, then an attacker could view and download the db's .gz and extract the user hashes, messages, smtp creds and more. Since the passwords are required to be strong by default, and hashed, it would prevent an attacker from easily obtaining passwords..but could be done offline with time and a powerful GPU/CPU.

Patches

Upgrade to version 4.0.4 or above

For more information

If you have any questions or comments about this advisory:

- #993
- #994

Severity

Moderate

CVE ID

CVE-2021-32630

Weaknesses

No CWEs