Advisory 2021-02 Potential Sensitive Data Exposure in FileCloud Versions 15 through 20.3.1

Potential Sensitive Data Exposure in FileCloud

Security Advisory Date	February 15, 2021
Vulnerability Type	Sensitive Data Exposure (for more information, see https://owasp.org/www-project-top-ten/)
Severity factors	Agent must be able to log in to the local network
Versions affected	FileCloud Version 15 through FileCloud Version 20.3.1
Version fixed	FileCloud Version 20.3.2.13174

Description

The security issue involved users whose folder permissions in FileCloud denied them access to a folder's sub-folders, but whose share permissions allowed them access to the same folder's sub-folders. Since these users could see actions on the sub-folders in their activity streams, they were able to view the names (but not the content) of the sub-folders and the files and folders they contained. If sub-folders or their files were named using confidential information, unauthorized users could see the confidential information, and in this way, it would be shared and possibly exploited.

Fix

This has been fixed in FileCloud version 20.3.2.13174 so that users who are not given access to sub-folders cannot see the sub-folder names.

What you should do

- If you are using a FileCloud on-premise installation, please update it to the latest version, which is 20.3.2.13174 or greater.
- If you are using FileCloud online, your site has already been updated to the latest version.

If you have any questions about this advisory, please contact FileCloud support.