Advisory 2021-09 Upload of Potentially Unsafe File Types

Threat of Remote Code Execution

Security Advisory Date	September 15, 2021
Vulnerability Type	Remote Code Execution
Severity factors	Medium, because upload of most potentially harmful file types are already blocked by FileCloud, and attackers must gain unauthorized access to the system.
Versions affected	All versions of FileCloud prior to 21.2.0.17160.
Version fixed	FileCloud Version 21.2.0.17160.

Description

Attackers with unauthorized admin privileges in FileCloud may have the ability to remotely access and control the FileCloud server, its databases, and its files by uploading files with .phtml and .phar extensions.
The latest version of FileCloud fixes this by prohibiting upload of .phtml and .phar files

Fix

This has been fixed in FileCloud version 21.2.0.17160, which blocks upload of .phtml and .phar files.

What you should do

- If you are using FileCloud on-premises, it is recommended that you update to the latest version, which is 21.2.0.17160 or greater. This will resolve the issue.
- If you are using FileCloud on-premises and do not upgrade to version 21.2.0.17160 or greater, perform the following steps to resolve the issue:
    1. In the FileCloud Admin portal, go to **Settings > Misc > General**.
    2. In **Disallowed File Extensions**, add **|phar|phtml**
    3. Click **Save.**
- 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.