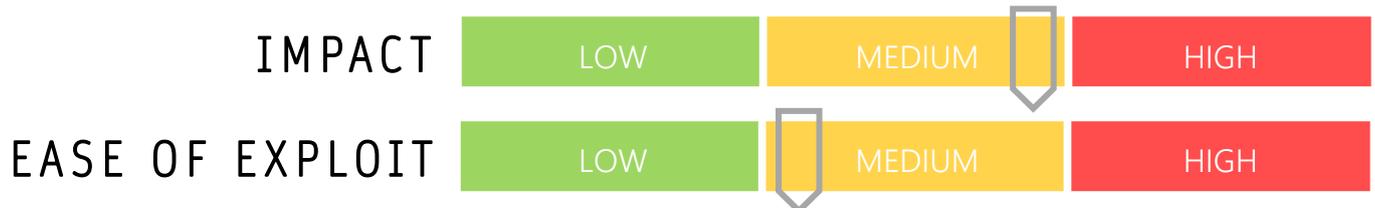


# CYBER GUIDANCE ISSUE 00029

## FILE MANAGER PLUGIN WORDPRESS FLAW

DATE ISSUED: 2<sup>nd</sup> September 2020



### OVERVIEW

With 700,000 active installations of the File Manager plugin for popular website host WordPress, under active exploitation by hackers, this flaw allows injection and execution of malicious scripts in files that contain webshells hidden in images

### BREAKDOWN

Numerous attempts have been detected over a number of sites and include the attempted upload of files sharing a common naming convention of hardfork.php, hardfind.php, and x.php. Commands are being run from the directory that stores the File Manager plugin (plugins/wp-file-manager/lib/files/). The problem occurs through the renaming of the elFinder element connector.minimal.php.dist. Those who breach the victim’s site often do so through compromised credentials are also able to escalate their privileges to administrator levels. This flaw affects versions 6.0 to 6.8 and WordPress have disclosed that 52% of current installations are at risk.

### REMEDIATION STEPS

- Sites running versions of File Manager mentioned above should upgrade to version 6.9 as soon as possible
- If you suspect your account may have been breached, reset your password
- Check and restrict access to multiple users where necessary

### REFERENCES & RESOURCES

ARS Technica: <https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/information-technology/2020/09/hackers-are-exploiting-a-critical-flaw-affecting-350000-wordpress-sites/?amp=1>

Security Affairs: <https://securityaffairs.co/wordpress/107826/hacking/file-manager-wordpress-plugin-flaw.html>

The Daily Swig: <https://portswigger.net/daily-swig/wordpress-security-zero-day-flaw-in-file-manager-plugin-actively-exploited>