Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:103 **10-Sep-2020**

Name: Zero-Day Vulnerability in WordPress File Manager Plugin

Threat Classification: Remote Code Execution

Affected Systems: Affects the following versions of File Manager Plugin:

- 6.0 to 6.8

Summary:

Security researchers have discovered that millions of WordPress sites have been probed and attacked by hackers due to a zero-day vulnerability in "File Manager", a popular WordPress plugin. The zero-day is an unauthenticated file upload vulnerability that allows an attacker to upload malicious files on a site running an older/ vulnerable version of the File Manager plugin. The developer team has created and released a patch for the zero-day.

Attack type	**0-day**
Attack Severity	**CRITICAL**
Attack Vector	Network
Privileges required	None

For further details, please visit following link:

https://www.wordfence.com/blog/2020/09/700000-wordpress-users-affected-by-zero-day-vulnerability-in-file-manager-plugin/

Recommendations:

- It is strongly recommended to update the File manager plugin to the latest version, currently version 6.9, immediately.
- Please look for below mentioned, top reported offending IP Addresses in your site's log files:
  1. 185.222.57.183
  2. 185.81.157.132
  3. 185.81.157.112
  4. 185.222.57.93
  5. 185.81.157.177
  6. 185.81.157.133
- When using utility plugins like this file manager plugin, it is recommended to take the utmost precaution. Plugins contain several features that if exposed within the admin area of WordPress installation, could cause serious problems.
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- Whenever required, run software with minimal access rights and privileges.
- Designate a PoC from your Security/ Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.