WordPress Plugin WP File Manager - Reflected XSS

Feb 26, 2021
3 minutes read

TL;DR

I have found an authenticated Reflected XSS on WordPress Plugin WP File Manager version <= 7.0 on the **User-Agent** HTTP parameter.

Plugin Information

- **Organization Name:** WP File Manager 7.0
- **Web Page:** https://wordpress.org/plugins/
- **Email:** plugins@wordpress.org
- **Vulnerability Disclosure Info or Technical Support Web Page:** https://filemanagerpro.io/contact/
- **Plugin name:** WP File Manager
- **Plugin version:** <= 7.0
- **Plugin Web Page:** https://wordpress.org/plugins/wp-file-manager/

WP File Manager is a popular WordPress plugin which makes very easy to manage files on a WordPress instance. It is currently used by 600,000+ active installations.

During a quick security auditing of the product, I have found that in the default configuration a Reflected XSS can occur on the endpoint /wp-admin/admin.php?page=wp_file_manager_properties when a payload is submitted on the **User-Agent** parameter. The payload is then reflected back on the web application response.

The fix was developed with the release 7.1, two days my vulnerability disclosure, which is a very good and serious way to handle security issues.

Vulnerability Details

Improper Neutralization of Input During Web Page Generation (Reflected Cross-Site Scripting) - CWE-79

- **Summary:** An authenticated remote user is able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Reflected Cross-Site Scripting attack against the platform administrators.
- **Prerequisites:** The plugin needs to be installed and activated on WordPress. No special configuration is required to reproduce the issue.
- **CVE and CVSS Score:** CVE-2021-24177 | **5.4** (Medium)

Step-by-step instructions and PoC

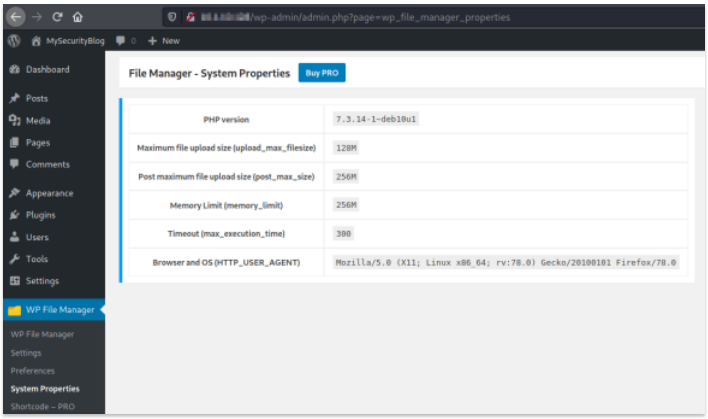
A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims.

Affected Endpoints:

- **URL:** http://wordpress/wp-admin/admin.php?page=wp_file_manager_properties
- **HTTP Parameter:** User-Agent

Below are the evidences with the vulnerability details and the payloads used.

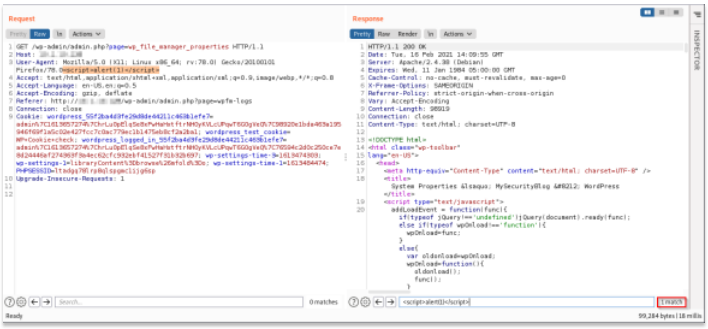
While the administrator user is logged in to WordPress, visit the **System Properties** page.



With the HTTP Proxy like Burp Suite intercept the request.
Then, repeat the request and append the following basic payload on `User-Agent` header:

```
<script>alert(1)</script>
```

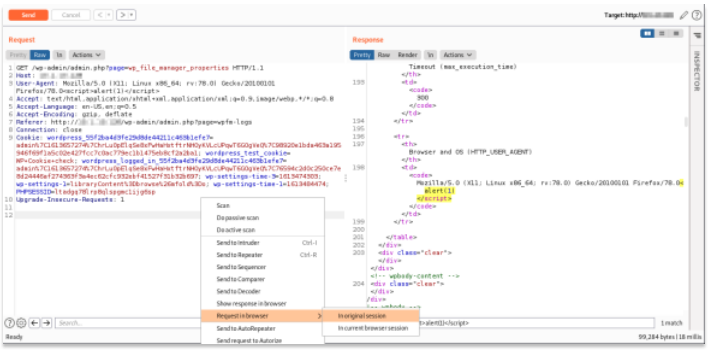
The payload is reflected on the response.



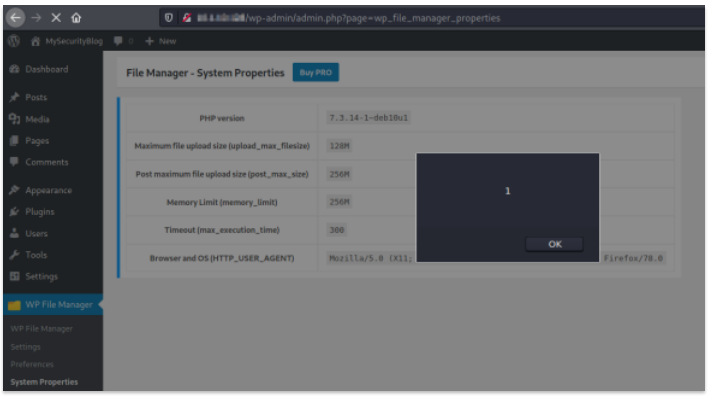
To weaponize the attack a malicious user can build a page which sends an XMLHTTPRequest on behalf of the user.
To simulate this behavior, *right-click* the HTTP request -> **Request in browser** -> **In original session**

Copy and paste an URL similar to the following:

```
http://burpsuite/repeat/2/0jmlsl04hq2916k69iae7rtharty29hu
```



To execute the JavaScript payload in the browser context, paste the URL in the browser:



Please note that the **/wp-admin/admin.php?page=wp_file_manager_properties** page is only available to WordPress administrators. Lower privileged users are not affected because the page is forbidden for them (error 403).

Security Impact

By exploiting this issue an attacker is able to target administrator users who are able to access the plugin configuration page within the browser with several type of direct or indirect impacts such as stealing cookies (if the HttpOnly flag is missing from the session cookies), modifying a web page, capturing clipboard contents, keylogging, port scanning, dynamic downloads and other attacks. This type of reflected XSS does require user interaction.

Timeline

- **16/02/2021**: First disclosure via private ticket on the Technical Support Web Page.
- **17/02/2021**: Human acknowledge e-mail from Technical Support!
- **18/02/2021**: Released the version 7.1, which has the fix for the vulnerability. Very impressive...
- **18/02/2021**: Added version on changelog: https://wordpress.org/plugins/wp-file-manager/#developers
- **26/02/2021**: Update is given that the vulnerability is fixed on version 7.1.
- **11/03/2021**: WPScan as CNA reserved the CVE on MITRE.
- **09/04/2021**: NVD scored CVE-2021-24177 as **5.4** (Medium).

Pi-hole - Multiple Vulnerabilities

WordPress Plugin wpDataTables - Multiple Vulnerabilities