Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 354 **18-12-2024**

Name: Multiple WordPress Plugin Vulnerabilities

Threat Classification: Vulnerability

Affected Software / Services:

- Fancy Roller Scroller - Plugin – 1.4.0 and earlier versions
- FloristPress – Plugin – 7.2.0 and earlier versions
- WP Quick Shop – Plugin – 1.3.1 and earlier versions
- Staggs Product Configurator for WooCommerce – Plugin – 2.0.0 and earlier versions
- Connect Contact Form 7 to Constant Contact – Plugin - 1.4 and earlier versions
- LabelGrid Tools – Plugin – 1.3.58 and earlier versions
- GeoFlickr jbd7 – Plugin – 1.3 and earlier versions
- Simple Presenter – Plugin – 1.5.1 and earlier versions
- DX Dark Site – Plugin – 1.0.1 and earlier versions
- Projectopia – Plugin – 5.1.7 and earlier versions

Summary:

Several vulnerabilities have been identified in WordPress. These include critical issues involving Cross-Site Request Forgery (CSRF) that could lead to Stored Cross-Site Scripting (XSS) in specific plugins. Additionally, a severe Authentication Bypass vulnerability in another plugin allows attackers to bypass authentication. Other vulnerabilities involve improper input neutralization during web page generation. Successful exploitation of these vulnerabilities could compromise the security of user data and the integrity of the affected applications.

- **CVE-2024-54351 and CVE-2024-54337:** Cross-Site Request Forgery (CSRF) vulnerability in DevriX DX Dark Site and Tom Landis Fancy Roller Scroller allows Stored XSS.

- **CVE-2024-54336:** Authentication Bypass Using an Alternate Path or Channel vulnerability in Projectopia.
- **CVE-2024-54347, CVE-2024-54344, CVE-2024-54342, CVE-2024-54343, CVE-2024-54341, CVE-2024-54339 and CVE-2024-54340:** Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) vulnerability in multiple plugins.

Severity	High
Attack Vector	Cross-Site Scripting

Recommendations:

- Please refer to the official WordPress website for the latest version of each product/plugin. https://wordpress.org/plugins
- Keep all the systems and software's up to date with the latest security patches to prevent attackers from exploiting known vulnerabilities.