PTA Cyber Security Advisory No. 332 **20-09-2024**

Name: Multiple WordPress Plugins Vulnerabilities

Threat Classification: Vulnerability

Affected Software / Services:

- Timetics- AI-powered Appointment Booking with Visual Seat Plan and ultimate Calendar Scheduling Plugin for WordPress **<=** 1.0.21
- Build App Online plugin for WordPress **<=** 1.0.21
- GiveWP Plugin for WordPress **<=** 3.14.1

Summary:

Multiple vulnerabilities have been identified in WordPress plugins. **"CVE-2024-1094"** affects the Timetics AI-powered Appointment Booking and Calendar Scheduling Plugin, potentially allowing a remote attacker to bypass security restrictions due to a missing capability check in the **make_staff()** function. This could enable the attacker to grant unauthorized staff permissions by sending a specially crafted request. **"CVE-2023-7264"** involves the Build App Online plugin, which has a weak password reset mechanism that could be exploited by a remote attacker to reset passwords for arbitrary users. Additionally, **"CVE-2024-5932"** impacts the GiveWP Plugin, where a PHP object injection vulnerability allows a remote attacker to execute arbitrary code on the system through deserialization of untrusted input from the **give_title** parameter, enabling the injection and execution of PHP Objects.

Severity	High
Attack Vector	Cross-Site Scripting

Recommendations:

- Upgrade to the latest version of plugin for WordPress, available from the WordPress Plugin Directory.
  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.
- In case of any incident, please report to this office, through PTA CERT Portal and email.