Responsible Disclosure Report – RCE via Outdated WordPress Plugin

Author: Aathithya Shanmuga Sundaram
Date of Disclosure: April 2025
Affected System: *Institutional Web Platform (WordPress-Based)*
Severity: High – Remote Code Execution (RCE) Risk

1. Executive Summary

During an independent security assessment of an academic institution's web platform, a high-severity vulnerability was identified in a **deprecated and vulnerable WordPress plugin**.
Public documentation confirmed that the version in use contained an RCE flaw, allowing potential attackers to execute arbitrary commands on the server under certain conditions.

No exploitation was performed. Only non-intrusive verification steps were used.

2. Nature of the Vulnerability (Redacted)

The website was using outdated versions of multiple plugins, including one with a **publicly disclosed RCE vulnerability**.

Examples of outdated plugins included:

- **Revolution Slider (RevSlider)**
- **WPBakery / Visual Composer (js_composer)**
- Additional legacy components with known CVEs

Specific version numbers, exploit chains, and payload details have been intentionally omitted.

3. Potential Impact

If exploited, the vulnerability could allow an attacker to:

- Execute arbitrary commands on the hosting environment
- Upload or modify malicious files
- Gain administrative-level control over the site
- Deface content or alter critical academic information
- Pivot to internal systems depending on configuration

This represents one of the highest risks for any public-facing platform.

4. How the Issue Was Identified

The assessment included:

- Reviewing plugin lists and version disclosures
- Cross-referencing with public CVE databases
- Validating signs of unmaintained components
- Observing backend references via sitemap and robots.txt

All verification was performed **without exploitation**.

5. Recommendations

- Immediately update or remove deprecated plugins
- Add automated dependency monitoring
- Restrict access to administrative plugin directories
- Enforce least-privilege configurations for web components
- Conduct recurring security audits on CMS installations

6. Author Statement

This report is provided in good faith to help strengthen the institution's web security posture. No exploitation or system modification was performed.

– Aathithya Shanmuga Sundaram
Responsible Disclosure Contributor