1. **WordPress Elementor DOM Reflected XSS**

|  |  |
| --- | --- |
| **Severity** |  |
| **CVSS Score** |  | **CVSS Vector** |  |
| **Affected URL** |  | | |
| **Reference URL** |  | | |

**Vulnerability Summary**

The Elementor Website Builder WordPress plugin prior to version 3.0.15 or lower does not sanitize or escape the user input appended to the DOM via a malicious payload, resulting in a DOM-based Reflected Cross-Site Scripting (XSS) vulnerability.

**Reproduction Steps**

**PoC**

**Impacts**

**Mitigations**

Upgrade the Elementor to the latest version 3.1.14.