July 11, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released update by Wordfence to address a critical vulnerability in the following product:

- InstaWP Connect

Technical Details

The InstaWP Connect – 1-click WP Staging & Migration plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 0.1.0.44. This is due to insufficient verification of the API key. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username, and to perform a variety of other administrative tasks. NOTE: This vulnerability was partially fixed in 0.1.0.44, but was still exploitable via Cross-Site Request Forgery.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- **CVE-2024-6397**
- **https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.0.43/includes/apis/class-instawp-rest-api.php#L256**
- **https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.0.43/includes/class-instawp-hooks.php#L28**
- **https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.0.43/includes/class-instawp-hooks.php#L40**
- **https://plugins.trac.wordpress.org/changeset/3109305/**
- **https://plugins.trac.wordpress.org/changeset/3114674/**
- **https://www.wordfence.com/threat-intel/vulnerabilities/id/963f2485-3afa-4e17-8278-b75415af3915?source=cve**