December 19, 2023

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that WordPress published security advisories to address vulnerabilities in all versions.

Technical Details

A critical severity vulnerability in a WordPress plugin with more than 90,000 installs can let attackers gain remote code execution to fully compromise vulnerable websites.

Known as Backup Migration, the plugin helps admins automate site backups to local storage or a Google Drive account. It impacts all plugin versions up to and including Backup Migration 1.3.6, and malicious actors can exploit it in low-complexity attacks without user interaction. CVE-2023-6553 allows unauthenticated attackers to take over targeted websites by gaining remote code execution through PHP code injection via the /includes/backup-heart.php file. This is due to an attacker being able to control the values passed to an include, and subsequently leverage that to achieve remote code execution. This makes it possible for unauthenticated threat actors to easily execute code on the server," Wordfence said on Monday.

"By submitting a specially-crafted request, threat-actors can leverage this issue to include arbitrary, malicious PHP code and execute arbitrary commands on the underlying server in the security context of the WordPress instance."

In the /includes/backup-heart.php file used by the Backup Migration plugin, an attempt is made to incorporate bypasser.php from the BMI_INCLUDES directory (defined by merging BMI_ROOT_DIR with the includes string) at line 118.

However, BMI_ROOT_DIR is defined through the content-dir HTTP header found on line 62, thereby making BMI_ROOT_DIR subject to user control.
These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-6553
- Nex Team
- 50K WordPress sites exposed to RCE attacks by critical bug in backup plugin (bleepingcomputer.com)