Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Information Security News

Date of Issue: 12 December 2023

50K Wordpress Sites Exposed to Remote Code Execution Attacks by Critical Bug in Back Up Plugin

Severity Level: High

Description:

A critical severity vulnerability has been identified in a WordPress plugin with more than 90,000 installs and this could be exploited by attackers to 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. The security bug (CVE-2023-6553) was discovered by a team of bug hunters known as Nex Team, who reported it to WordPress security firm Wordfence under a recently launched bug bounty program.

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.

As per Wordfence, 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. 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.

Wordfence reported the critical security flaw to BackupBliss, the development team behind the Backup Migration plugin, on December 6, with the developers releasing a patch hours later.

However, despite the release of the patched Backup Migration 1.3.8 plugin version on the day of the report, almost 50,000 WordPress websites using a vulnerable version still have to be secured nearly one week later, as WordPress.org org download stats show.

References

https://www.bleepingcomputer.com/news/security/50k-wordpress-sites-exposed-to-rce-attacks-by-critical-bug-in-backup-plugin/

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org