Corvit Systems Multan

Report Title:

CVE-2024-25600: WordPress Bricks Builder Remote Code Execution

Course: CEH (Certified Ethical Hacking)

Submitted By: M. Adnan Shakeel

Submitted To: Supervisor M. Bilal

Date: 18/08/2024

CVE-2024-25600: WordPress Bricks Builder Remote Code Execution Vulnerability

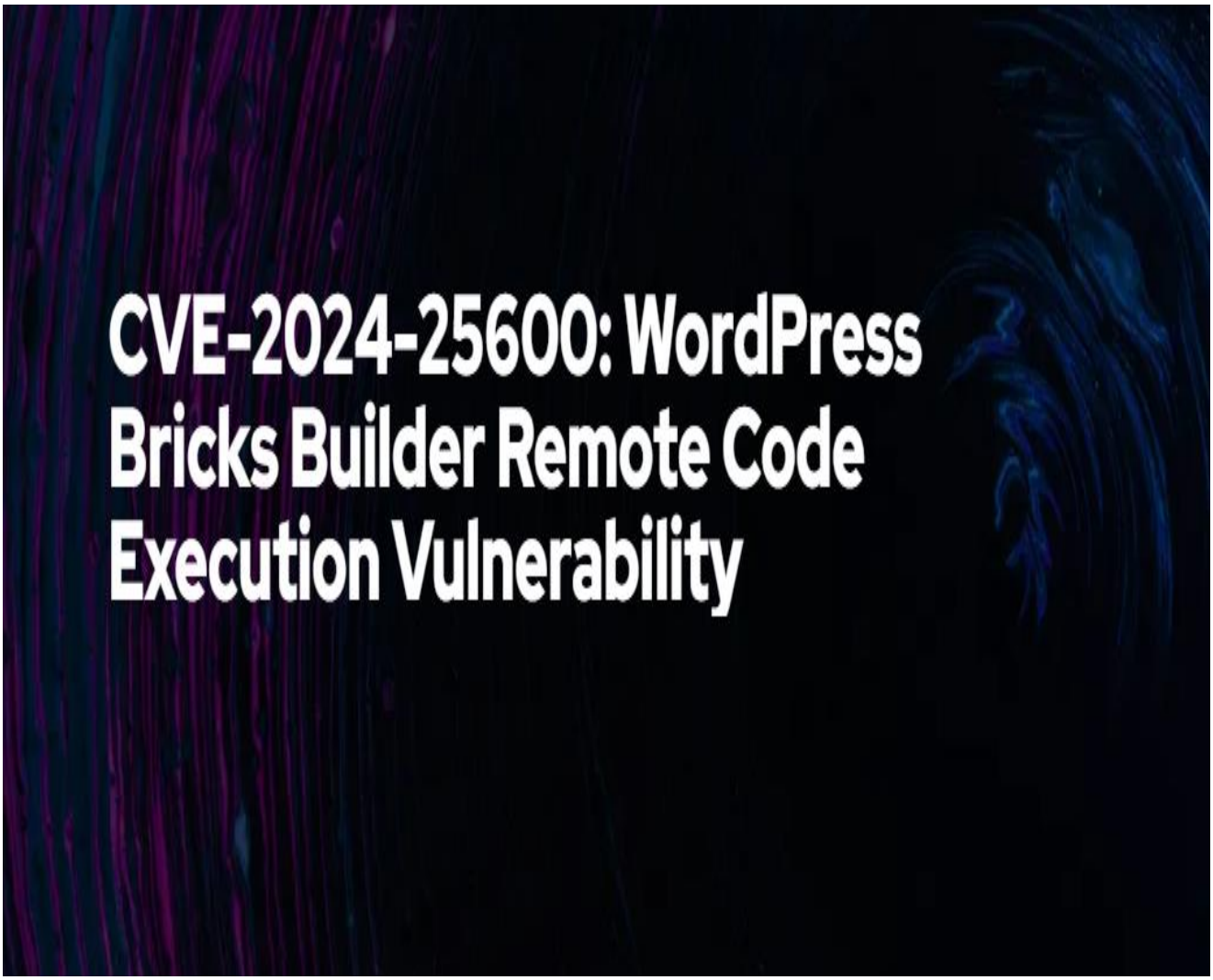

Table of Contents

Topics page

Vulnerability Details

CVE ID:	CVE-2024-25600
Release Date	February 26, 2024
Component Name	Bricks Builder
Affected Versions	Bricks Builder ≤ 1.9.6
Vulnerability Type	Remote Code Execution Vulnerability
Severity	**CVSS v3 Base Score:** 9.8 (Critical)

Description:

Bricks Builder is a popular WordPress development theme with approximately 25,000 active installations. It provides an intuitive drag-and-drop interface for designing and building WordPress websites.

The vulnerability allows unauthenticated attackers to execute arbitrary code on the server hosting the WordPress site. This can lead to various malicious activities, including:

- Installing malware or backdoors
- Stealing sensitive data
- Defacing the website
- Using the server for further attacks

Impact

The impact of CVE-2024-25600 is severe due to several factors:

- **Unauthenticated Access:** The exploit can be carried out without any authenticated session or user credentials, making every website running a vulnerable version of the Bricks Builder plugin an easy target.
- **Remote Code Execution:** Successful exploitation allows attackers to execute arbitrary code on the server, providing the capability to modify website content, steal sensitive data, and gain unauthorized access to the hosting environment.
- **Widespread Risk:** Given the popularity of the Bricks Builder plugin among WordPress users for its design flexibility, a significant number of websites are at risk until patched.

Active Exploitation:

Security experts at Wordfence have confirmed multiple attacks targeting CVE-2024-25600 in the last 24 hours. The attacks have originated from several IP addresses, including but not limited to:

- 200.251.23.57
- 92.118.170.216
- 103.187.5.128
- 149.202.55.79
- 5.252.118.211
- 91.108.240.52

Additionally, malware specifically designed to exploit this vulnerability has been observed, with features to disable security-related plugins such as Wordfence and Sucuri.

Mitigation:

- Bricks Builder has released a patch (version 1.9.6.1) to address this vulnerability. It is imperative that all users of Bricks Builder update to this version immediately to secure their sites. Delaying the update increases the risk of exploitation.
- Updating Bricks Builder can typically be done directly within your WordPress dashboard. For detailed instructions, refer to the Bricks Builder website or their official documentation.

Recommendations:

- **Immediate Action:** Update Bricks Builder to version 1.9.6.1 without delay.
- **Monitor:** Keep an eye on your website for any suspicious activity and regularly check for updates and patches for all installed themes and plugins.
- **Security Measures:** Ensure that your website is protected with robust security measures, including firewalls, security plugins, and regular backups.

References

Hyperlink
https://github.com/Chocapikk/CVE-2024-25600
https://github.com/K3ysTr0K3R/CVE-2024-25600-EXPLOIT
https://patchstack.com/articles/critical-rce-patched-in-bricks-builder-theme?_s_id=cve
https://patchstack.com/database/vulnerability/bricks/wordpress-bricks-theme-1-9-6-unauthenticated-remote-code-execution-rce-vulnerability?_s_id=cve
https://snicco.io/vulnerability-disclosure/bricks/unauthenticated-rce-in-bricks-1-9-6

Conclusion:

The CVE-2024-25600 vulnerability in WordPress's Bricks Builder is a critical threat that requires immediate attention. By promptly updating to the patched version and maintaining vigilant security practices, you can protect your website from potential exploitation and ensure the safety of your digital assets