Assignment # 4

Presented By

Arsalan Akmal

TOPIC

CVE-2024-25600:

Code Execution Vulnerability

CVE-2024-25600 - WordPress Bricks Builder Remote Code Execution (RCE)

The Bricks theme for WordPress has been identified as vulnerable to a critical security flaw known as CVE-2024-25600. This vulnerability affects all versions up to, and including, 1.9.6 of the Bricks Builder plugin. It poses a significant risk as it allows unauthenticated attackers to execute arbitrary code remotely on the server hosting the vulnerable WordPress site. CVE-2024-25600 is classified under Remote Code Execution (RCE) vulnerabilities, enabling attackers to manipulate the server into executing malicious code without any authentication. This vulnerability exploits a flaw in the Bricks Builder plugin's handling of user input, allowing attackers to inject and execute PHP code remotely. The exploitation of this vulnerability can lead to full site compromise, data theft, and potential spreading of malware to site visitors.

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.

Mitigation Steps

To mitigate the risk posed by CVE-2024-25600, website administrators and security teams should immediately take the following steps:

- **Update the Plugin:** Upgrade the Bricks Builder plugin to the latest version immediately. The developers have released patches addressing this vulnerability in versions following 1.9.6.
- **Security Review:** Conduct a thorough security review of your website to ensure no unauthorized modifications have been made.

- **Regular Monitoring:** Implement regular monitoring of web logs for any suspicious activity that could indicate exploitation attempts or successful breaches.
- **Security Best Practices:** Adhere to security best practices for WordPress sites, including using strong passwords, limiting login attempts, and using security plugins to monitor and protect your site.

Disclaimer

Here's a Proof of Concept (PoC) for educational and security research purposes only. The use of the information provided is at your own risk. The author or contributors do not encourage unethical or illegal activity. Ensure you have explicit permission before testing any system with the techniques and code described.

1. About the Vulnerability

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

2. About CVE-2024-25600

2.1 About the Component

Bricks Builder is a development theme for WordPress developed by Bricks. It provides an intuitive drag-and-drop interface for designing and building WordPress websites.

2.2 About the Vulnerability

On February 26, 2024, Sangfor FarSight Labs received notification of the remote code execution vulnerability (CVE-2024-25600) in Bricks Builder, classified as critical (CVSS Score 9.8). This vulnerability is caused by the improper use of the eval function in PHP code within Bricks Builder. Attackers can exploit this vulnerability by crafting malicious data to execute remote code without authorization, thereby taking over the server.

3. Affected Versions

Bricks Builder ≤ 1.9.6

4. Solutions

4.1 Remediation Solutions

4.1.1 Official Solution

Bricks has released a new version of Bricks Builder, and affected users are strongly recommended to update to the latest version to fix the vulnerability. For more information, visit https://bricksbuilder.io/

4.2 Sangfor Solutions

4.2.1 Security Monitoring

The following Sangfor products and services perform **real-time monitoring of assets affected** by the WordPress Bricks Builder remote code execution vulnerability (CVE-2024-25600):

- Sangfor Cyber Command (Network Detection and Response)
- Sangfor Cyber Guardian (Managed Detection and Response)

4.2.2 Security Protection

The following Sangfor products and services **provide protection against** the WordPress Bricks Builder remote code execution vulnerability (CVE-2024-25600):

- Sangfor Network Secure (Next-Generation Firewall)
- Sangfor Cyber Guardian (Managed Detection and Response)

5. Timeline

On February 26, 2024, Sangfor FarSight Labs received notification of the WordPress Bricks Builder remote code execution vulnerability (CVE-2024-25600).
On February 26, 2024, Sangfor FarSight Labs released a vulnerability alert.
On February 28, 2024, Sangfor FarSight Labs released remediation solutions.

6. References

https://snicco.io/vulnerability-disclosure/bricks/unauthenticated-rce-in-bricks-1-9-6

7. About Sangfor FarSight Labs

Sangfor FarSight Labs researches the latest cyberthreats and unknown zero-day vulnerabilities, alerting customers to potential dangers to their organizations, and providing real-time solutions with actionable intelligence. Sangfor FarSight Labs works with other security vendors and the security community at large to identify and verify global cyberthreats, providing fast and easy protection for customers.