مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability- Critical RCE flaw in Bricks WordPress site builder

Tracking #:432315631

Date:20-02-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE The Cyber Security Council has observed threat actors actively exploiting a critical remote code execution (RCE) flaw in the Bricks Builder Theme for WordPress to run malicious code on vulnerable sites.

TECHNICAL DETAILS:

A critical remote code execution (RCE) flaw exists in the Brick Builder Theme for WordPress. Threat actors are actively exploiting this vulnerability to execute malicious PHP code on vulnerable websites. The vulnerability is tracked as **CVE-2024-25600 (CVSS score: 9.8 CRITICAL)** and affects installations of the Brick Builder Theme using its default configuration. The security issue arises from an eval function call within the prepare_query_vars_from_settings function, which could allow an unauthenticated user to exploit it to execute arbitrary PHP code.

Successful exploitation of this vulnerability could allow unauthenticated attackers to execute arbitrary code on affected websites, potentially leading to complete site takeover, data theft, or malware injection.

Affected Versions:
Bricks Builder Theme for WordPress (versions prior to 1.9.6.1)

Fixed Versions:
Bricks Builder Theme for WordPress (versions 1.9.6.1 or Higher)

INDICATORS OF COMPROMISE(IOCs):

- 200.251.23[.]57
- 92.118.170[.]216
- 103.187.5[.]128
- 149.202.55[.]79
- 5.252.118[.]211
- 91.108.240[.]52

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Bricks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://patchstack.com/articles/critical-rce-patched-in-bricks-builder-theme/