Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

20 February 2024

WordPress Bricks Builder Vulnerability

CVE-2024-25600 | Active Exploitation | RCE | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerability under active exploitation known as CVE-2024-25600.[1] The vulnerability affects WordPress plugin Bricks Builder versions 1.9.6 and lower.[2] An unauthenticated attacker may exploit the vulnerability via unauthenticated remote code execution (RCE), allowing the attacker to run arbitrary commands and take over the site/serve.[3]

The Cal-CSIC recommends immediately upgrading to Bricks Builder version 1.9.6.1 or higher.

For further information on applying upgrades, please refer to Bricks Builder 1.9.6.1 Changelog.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Snicco; "Unauthenticated Remote Code Execution – Bricks <= 1.9.6;" https://snicco.io/vulnerability-disclosure/bricks/unauthenticated-rce-in-bricks-1-9-6; accessed 20 February 2024

[2] Bleeping Computer; "Hackers exploit critical RCE flaw in Bricks WordPress site builder;" https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-rce-flaw-in-bricks-wordpress-site-builder/; accessed 20 February 2024

[3] SC Media; "WordPress plugin under attack; Bricks Builder bug enables RCE;" https://www.scmagazine.com/news/wordpress-plugin-under-attack-bricks-builder-bug-enables-rce; accessed 20 February 2024