CYBER ADVISORY

TLP:CLEAR

14 October 2024

Gutenkit for Gutenberg Block Editor WordPress Plugin Vulnerability

CVE-2024-9234 | Wordpress | Arbitrary Upload | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-9234. The Gutenkit vulnerability affects all versions up to and including 2.1.0.[1][2] Exploitation of the arbitrary file upload function may allow a remote unauthenticated attacker to install and activate arbitrary plugins or utilize the functionality to upload arbitrary files spoofed as plugins.[3]

The Cal-CSIC recommends immediately upgrading to Gutenkit 2.1.1.

For further information on applying upgrades please refer to Wordpress Plugin Installation.

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.
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] National Vulnerability Database. (2024). *CVE-2024-9234*. National Institute of Standards and Technology. "https://nvd.nist.gov/vuln/detail/CVE-2024-9234" accessed on 14OCT24

[2] GitHub Security Advisories. (2024). *GHSA-7cmx-277j-7rf8*. "https://github.com/advisories/GHSA-7cmx-277j-7rf8" accessed on 14OCT24

[3] Wordfence. (2024). *Unauthenticated arbitrary file upload vulnerability in GutenKit Blocks Addon plugin* (v2.1.0). "https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/gutenkit-blocks-addon/gutenkit-210-unauthenticated-arbitrary-file-upload"; accessed on 14OCT24