CYBER ADVISORY

TLP:CLEAR

09 January 2024

WordPress BERTHA AI plugin Vulnerability

CVE-2023-51419 | Arbitrary File Upload | WordPress | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-51419.[1] The vulnerability affects the WordPress BERTHA AI plugin version 1.11.10.7.[2] Exploitation of this vulnerability could allow an attacker to upload arbitrary files, including potentially malicious PHP files, which could lead to remote code execution on the affected system.[3,4]

The Cal-CSIC recommends immediately upgrading to WordPress BERTHA AI plugin version 1.11.10.8.

For further information on applying patches, please refer to WordPress vulnerability database.

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 here.

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; "CVE-2023-51419 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2023-51419; accessed 09 January 2024
[2] Security Online; "The Severe Vulnerability Threatening 50000 Wordpress Sites;" https://securityonline.info/cve-2023-51409-the-severe-vulnerability-threatening-50000-wordpress-sites/; accessed 09 January 2024
[3] Patchstack; "AI Engine Plugin Affected by Critical Vulnerability;" https://patchstack.com/articles/ai-engine-plugin-affected-by-critical-vulnerability/; accessed 09 January 2024
[4] Info Security Magazine; "Flaw in AI Plugin Exposes 50,000 WordPress Sites to Remote Attack;" https://www.infosecurity-magazine.com/news/flaw-ai-plugin-exposes-50000-wp/; accessed 09 January 2024