CYBER ADVISORY

TLP:CLEAR
29 February 2024

WordPress WPvivid Vulnerability

CVE-2024-1981 | SQL Injection | WPvivid | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-1981.[1] The vulnerability affects WordPress plugin WPvivid Backup and Migration version 0.9.68 and likely lower.[2] The vulnerability is present due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This may allow an unauthenticated attacker to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.[3]

The Cal-CSIC recommends immediately upgrading to WPvivid version 0.9.69 or higher.

For further information on applying upgrades, please refer to WPvivid Backup & Migration.

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] National Vulnerability Database; "CVE-2024-1981 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-1981; accessed 29 February 2024

[2] HiSolutions; "Multiple vulnerabilities in WordPress Plugin – WPvivid Backup and Migration;" https://research.hisolutions.com/2024/01/multiple-vulnerabilities-in-wordpress-plugin-wpvivid-backup-and-migration/; accessed 29 February 2024

[3] Wordfence; "WPvivid Backup and Migration <= 0.9.68 - Unauthenticated SQL Injection;" https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wpvivid-backuprestore/wpvivid-backup-and-migration-0968-unauthenticated-sql-injection; accessed 29 February 2024

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.