CYBER ADVISORY

TLP:CLEAR
02 May 2024

PowerPanel Vulnerabilities

CVE-2024-34025 | CVE-2024-32053 | CVE-2024-32047 | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of critical vulnerabilities known as CVE-2024-34025, CVE-2024-32053, and CVE-2024-32047.[1] The vulnerabilities affect CyberPower's PowerPanel Business for Windows, versions 4.9.0 and prior. PowerPanel is software that features an interface for controlling and monitoring any CyberPower UPS system.[2] Exploitation of CVE-2024-34025 may allow an attacker forging JWT tokens to bypass authentication. Exploitation of CVE-2024-32053 may allow an attacker to gain access to services with the privileges of a Powerpanel application. Exploitation of CVE-2024-32047 may allow an attacker to gain access to the testing or production server.

The Cal-CSIC recommends immediately upgrading to PowerPanel Business for Windows version 4.10.1 or later.

For further information on applying PowerPanel upgrades, please refer to PowerPanel Business for Windows.

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] CISA; "CyberPower PowerPanel;" https://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01; accessed 02 May 2024

[2] CyberPower Systems; "Powerpanel Business Software;" https://www.cyberpowersystems.com/products/software/power-panel-business/; accessed 02 May 2024