CYBER ADVISORY UPDATE

TLP:CLEAR
17 December 2024

CyberPanel Vulnerability Update

CyberPanel | Command Injection | Bypass Security | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of new information regarding CVE-2024-51378. This vulnerability affects CyberPanel, an open-source free web hosting server control panel that includes website, domain, and email management tools. Since the date of publication of our previous Cyber Advisory (serial number 202410-010), two more ransomware groups, Babuk and Conti, are reportedly encrypting CyberPanel instances[1],[2]. These groups are in addition to the previously reported PSAUX ransomware group. Additionally, CISA has added CVE-2024-51378 to its Known Exploited Vulnerabilities (KEV) catalog[3].

The Cal-CSIC recommends immediately updating to the latest CyberPanel version.

For further information on applying updates please refer to Cyber Panel Documentation.

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	**UPDATE THIS PORTION APPROPRIATELY**
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] GitHub Gist; "CyberPanel ransomware attack/defense" https://gist.github.com/gboddin/d78823245b518edd54bfc2301c5f8882; accessed 16 December 2024
[2] Censys; "November 1 Advisory: CyberPanel RCE Leveraged for Ransomware [CVE-2024-51November 1 Advisory: CyberPanel RCE Leveraged for Ransomware [CVE-2024-51378]378]" https://censys.com/cve-2024-51378/; accessed 16 December 2024
[3] Cybersecurity and Infrastructure Security Agency; "Known Exploited Vulnerabilities Catalog" https://www.cisa.gov/known-exploited-vulnerabilities-catalog; accessed 16 December 2024