CYBER ADVISORY

TLP:CLEAR
31 October 2024

Multiple Zero-day CyberPanel Vulnerabilities

CyberPanel | Command Injection | Bypass Security | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of three critical vulnerabilities known as CVE-2024-51378,[1] CVE-2024-51567,[2] and CVE-2024-51568[3]. These vulnerabilities in CyberPanel are present in versions 2.3.6 and potentially 2.3.7. Each of these vulnerabilities carries a maximum CVSS version 3.x score of 10, indicating severe risk[4]. CyberPanel is an open-source free web hosting server control panel that includes website, domain, and email management tools. CVE-2024-51378 allows for the bypass of authentication and to conduct remote code execution (RCE). CVE-2024-51567 similarly bypasses authentication and allows for the execution of arbitrary commands. Lastly, CVE-2024-51568 enables command injection in the ProcessUtilities.outputExecutioner() function, specifically through the completePath parameter. These vulnerabilities continue to be exploited in the on-going PSAUX ransomware campaign[5].

The Cal-CSIC recommends immediately updating to the latest Cyber Panel 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	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-2024-51378 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-51378; accessed 30 October 2024
[2] National Vulnerability Database; "CVE-2024-51567 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-51567; accessed 30 October 2024
[3] National Vulnerability Database; "CVE-2024-51568 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-51568; accessed 30 October 2024
[4] SOCRadar; "Critical Flaws At CyberPanel Servers Exploitation Risk by PASAUX Ransomware" https://socradar.io/over-22000-cyberpanel-servers-at-risk-from-critical-vulnerabilities-exploitation-by-psaux-ransomware/; accessed 31 October 2024
[5] Bleeping Computer; "Massive PSAUX ransomware attack targets 22,000 CyberPanel instances" https://www.bleepingcomputer.com/news/security/massive-psaux-ransomware-attack-targets-22-000-cyberpanel-instances/; accessed 31 October 2024