CYBER ADVISORY

TLP:CLEAR
6 November 2024

HP Access Point Command Injection Could Lead to RCE

Hewlett Packard | Command Injection | Access Points | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of one critical vulnerability known as CVE-2024-47460 with a CVSS 3.x score of 9.0.[1] This command injection vulnerability could lead to unauthenticated remote code execution (RCE) by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) over UDP port 8211. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. The following are the affected versions: AOS-10.4.1.4, Instant AOS-8.12.0.2 and lastly Instant AOS-8.10.0.13.[2]

The Cal-CSIC recommends immediately updating the affected access points to the latest HPE Aruba Networking version.

Alternately, enabling cluster security through the cluster-security command to prevent this vulnerability from being exploited in devices running Instant AOS-8 code. For AOS-10 devices access port UDP 8211 must be blocked from all untrusted networks.

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-2024-47460 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-47460; accessed 6 November 2024

[2] Hewlett Packard Enterprise; "Security Bulletin" https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US; accessed 6 November 2024