CYBER ADVISORY

TLP:CLEAR
15 May 2024

Multiple HPE Aruba Vulnerabilities

Aruba | Code Execution | High Vulnerabilities | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple high and critical vulnerabilities affecting HPE Aruba software.[1] Exploitation of the most critical of the vulnerabilities could provide an attacker with the ability to execute arbitrary commands as a privileged user on the underlying operating system.[2,3]

Affected Aruba Product(s)
ArubaOS 10.5.x.x: 10.5.1.0 and below
ArubaOS 10.4.x.x: 10.4.1.0 and below
InstantOS 8.11.x.x: 8.11.2.1 and below
InstantOS 8.10.x.x: 8.10.0.10 and below
InstantOS 8.6.x.x: 8.6.0.23 and below

Table 1: Vulnerable HPE Aruba Products

Issue	CVE Identifier(s)
Unauthenticated Buffer Overflow Vulnerabilities in CLI Service Accessed by the PAPI Protocol	CVE-2024-31466; CVE-2024-31467
Unauthenticated Buffer Overflow Vulnerabilities in Central Communications Service Accessed by the PAPI Protocol	CVE-2024-31468; CVE-2024-31469
Unauthenticated Buffer Overflow Vulnerability in the Simultaneous Authentication of Equals (SAE) Service Accessed by the PAPI Protocol	CVE-2024-31470
Unauthenticated Command Injection Vulnerability in Central Communications Service Accessed by the PAPI Protocol	CVE-2024-31471
Unauthenticated Command Injection Vulnerabilities in the Soft AP Daemon Service Accessed by the PAPI Protocol	CVE-2024-31472
Unauthenticated Command Injection Vulnerability in the Deauthentication Service Accessed by the PAPI Protocol	CVE-2024-31473
Unauthenticated Arbitrary File Deletion in CLI Service Accessed by the PAPI Protocol	CVE-2024-31474
Unauthenticated Arbitrary File Deletion in Central Communications Service Accessed by the PAPI Protocol	CVE-2024-31475
Authenticated Remote Command Execution in Aruba InstantOS or ArubaOS 10 Command Line Interface	CVE-2024-31476; CVE-2024-31477
Unauthenticated Denial-of-Service (DoS) Vulnerabilities in the Soft AP Daemon Service Accessed via the PAPI Protocol	CVE-2024-31478

Table 2: HPE Aruba Critical & High CVE List

TLP:CLEAR

The Cal-CSIC recommends to immediately apply the appropriate mitigations or updates for the affected Aruba product.

For further information on applying mitigations and/or updates, please refer to HPE Networking Support Portal.

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] Aruba Networks; "HPE Aruba Networking Product Security Advisory;" https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2024-006.txt; accessed 15 May 2024
[2] Tenable; "CVE-2024-31467;" https://www.tenable.com/cve/CVE-2024-31467; accessed 15 May 2024
[3] VulDB; "Aruba Instantos/Arubaos Papi Command Injection;" https://vuldb.com/?id.264382; accessed 15 May 2024

TLP:CLEAR