Advisory Alert

Alert Number: **AAA20241106** **Date:** **November 6, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Remote Arbitrary Command Execution Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Arbitrary Command Execution Vulnerabilities (CVE-2024-42509, CVE-2024-47460, CVE-2024-47461, CVE-2024-47462, CVE-2024-47463, CVE-2024-47464)
Description	HPE has released security updates addressing Remote Arbitrary Command Execution Vulnerabilities that exist in HPE Aruba Networking Access Points. Exploitation of these vulnerabilities may lead to system compromisation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking - Access Points running • AOS-10.4.x.x: 10.4.1.4 and below • Instant AOS-8.12.x.x: 8.12.0.2 and below • Instant AOS-8.10.x.x: 8.10.0.13 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.