TLP: CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2022-024

DATE(S) ISSUED:
02/28/2023

SUBJECT:
Multiple Vulnerabilities in Aruba Products Could Allow for Arbitrary Code Execution.

OVERVIEW:
Multiple vulnerabilities have been discovered in Aruba Products, the most severe of which could allow for Arbitrary code execution.

- Aruba Mobility Conductor is an advanced WLAN deployed as a virtual machine (VM) or installed on an x86-based hardware appliance.
- Aruba Mobility Controller is a WLAN hardware controller in a virtualized environment
- WLAN Gateways and SD-WAN Gateways managed by Aruba Central

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected service account. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Aruba OS versions prior to 8.6.0.20
- Aruba OS versions prior to 8.7.0.0-2.3.0.9
- Aruba OS versions prior to 8.10.0.5
- Aruba OS versions prior to 8.11.0.0
- Aruba OS versions prior to 10.3.1.1

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low
TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Aruba Products, the most severe of which could allow for Arbitrary code execution. Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001)

Technique: *Exploit Public-Facing Application* (T1190)

- Unauthenticated Stack-Based Buffer Overflow Vulnerabilities in the PAPI Protocol (CVE-2023-22751, CVE-2023-22752)
- Multiple Unauthenticated Command Injections in the PAPI Protocol (CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750)
- Unauthenticated Buffer Overflow Vulnerabilities in ArubaOS Processes (CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756, CVE-2023-22757)

Details of lower-severity vulnerabilities are as follows:

- Authenticated Read Buffer Overruns Processing ASN.1 Strings in ArubaOS (CVE-2021-3712)
- Authenticated Remote Command Execution in ArubaOS Web-based Management Interface (CVE-2023-22758, CVE-2023-22759, CVE-2023-22760, CVE-2023-22761)
- Authenticated Remote Command Execution in the ArubaOS Command Line Interface (CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769, CVE-2023-22770)
- Insufficient Session Expiration in ArubaOS Command Line Interface (CVE-2023-22771)
- Authenticated Path Traversal in ArubaOS Web-based Management Interface Allows for Arbitrary File Deletion. (CVE-2023-22772)
- Authenticated Path Traversal in ArubaOS Command Line Interface Allows for Arbitrary File Deletion. (CVE-2023-22773, CVE-2023-22774)
- Authenticated Sensitive Information Disclosure in ArubaOS Command Line Interface. (CVE-2023-22775)
- Authenticated Remote Path Traversal in ArubaOS Command Line Interface Allows for Arbitrary File Read (CVE-2023-22776)
- Authenticated Information Disclosure in ArubaOS Web-based Management Interface (CVE-2023-22777)
- Authenticated Stored Cross-Site Scripting (CVE-2023-22778)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected service account. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Aruba to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually,

or when significant enterprise changes occur that could impact this Safeguard.

- **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- **Safeguard 7.3: Perform Automated Operating System Patch Management:** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis
- **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently
- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. **(M1016: Vulnerability Scanning)**
    - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing.Penetration testing relies on the skill of the tester to

manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. **(M1030: Network Segmentation)**
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
- Restrict execution of code to a virtual environment on or in transit to an endpoint system. **(M1048: Application Isolation and Sandboxing)**
    - **Safeguard 16.8: Separate Production and Non-Production Systems:** Maintain separate environments for production and non-production systems.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection)**
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.

REFERENCES:

Aruba Networks:

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22747
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22753
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22755

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22756
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22769
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22771
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22773
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22778

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24×7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722