The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
10/17/2022

SUBJECT:
Multiple Vulnerabilities in Aruba EdgeConnect Enterprise Orchestrator Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Aruba EdgeConnect Enterprise Orchestrator's Web-Based Management Interface, the most severe of which could allow for remote code execution. Aruba EdgeConnect Enterprise Orchestrator is a widely used WAN management solution. Critical and easily exploitable flaws in this product introduce risks for systems and networks. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts 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:

- Orchestrator 9.1.2.40051 and below
- Orchestrator 9.0.7.40108 and below
- Orchestrator 8.10.23.40009 and below

RISK:
Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Aruba EdgeConnect Enterprise Orchestrator's Web-Based Management Interface, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

Tactic: *Execution* (TA0002):

Technique: *Exploitation for Client Execution* (T1203):

- A vulnerability in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host. In order for a threat actor to exploit these vulnerabilities, WAN access would need to be available for the CLI and/or web-based management interfaces. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. (CVE-2022-37915)

Tactic: *Initial Access* (TA0001)

Technique: *Exploitation for Privilege Escalation* (T1404)

- A vulnerability in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an unauthenticated remote attacker to bypass authentication. In order for a threat actor to exploit these vulnerabilities, WAN access would need to be available for the CLI and/or web-based management interfaces. Successful exploitation of these vulnerabilities could allow an attacker to gain administrative privileges leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host. (CVE-2022-37913, CVE-2022-37914)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts 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 7.4: 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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- 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™.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allow listing, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

REFERENCES:

Aruba EdgeConnect Enterprise Orchestrator:

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-015.txt

ArticWolf:
https://arcticwolf.com/resources/blog/critical-remote-code-execution-authentication-bypass-vulnerabilities-in-aruba-edgeconnect-enterprise-orchestrator/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37914
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37915