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

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

03/30/2021

SUBJECT:

Multiple Vulnerabilities in ArubaNetwork's Instant Access Point Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in ArubaNetwork's Instant Access Point that could allow for arbitrary code execution. Aruba (a Hewlett Packard Enterprise company) is the worldwide second-largest enterprise WLAN vendor. ArubaNetworks Instant Access Point is Wi-Fi hardware which virtualizes Aruba Mobility Controller capabilities on 802.11 access points (APs). Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application. 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:

- ArubaNetwork's Instant Access Point Versions: 6.4.0.0, 6.5.0.0, 6.4.4.8-4.2.4.17, 6.5.4.16-17, 8.3.0.0, 8.3.0.12-13, 8.5.0.0, 8.5.0.6-7, 8.5.0.10, 8.6.0.0, 8.6.0.2-3, 8.6.0.5, 8.7.0.0

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in ArubaNetwork's Instant Access Point, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- An authenticated command injection vulnerability exists in the Aruba Instant command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying access point operating system. (CVE-2020-24635, CVE-2021-25146)
- There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system. (CVE-2019-5319, CVE-2021-25144, CVE-2021-25149)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. 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:
The following actions should be taken:

- Block external access at the network boundary, unless external parties require service.
- Filter access to the affected computer at the network boundary if global access isn't needed. Restricting access to only trusted computers and networks might greatly reduce the likelihood of a successful exploit.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Deploy NIDS to detect and block attacks and anomalous activity such as requests containing suspicious network traffic.

REFERENCES:
Aruba:
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-007.txt

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5319
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25146
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25149