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:
06/16/2022

SUBJECT:
A Vulnerability in Cisco Email Security Appliance, Cisco Secure Email & Web Manager Could Allow for an Authentication Bypass

OVERVIEW:
A vulnerability in Cisco Email Security Appliance, Cisco Secure Email & Web Manager could Allow for an authentication bypass under specific conditions. Exploitation of this vulnerability could allow for an unauthenticated attacker to gain unauthorized access to the web-based management interface of the affected device.

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

SYSTEMS AFFECTED:

- Cisco Email Security Appliance, Cisco Secure Email & Web manager running a vulnerable release of Cisco AsyncOS software. Please review the referenced Cisco advisory for a detail list of affected software versions.

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:

A vulnerability in Cisco Email Security Appliance, Cisco Secure Email & Web Manager could Allow for an authentication bypass under specific conditions:

- The affected device enable the use of external authentication
- The affected device is utilizing LDAP as its authentication protocol

Tactic: *Initial Access* **(**TA0001**):**

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

- Improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication. (CVE-2022-20798)

Exploitation of this vulnerability could allow for an unauthenticated attacker to gain unauthorized access to the web-based management interface of the affected device.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Cisco to vulnerable systems immediately after appropriate testing. (**M1051: Update Software, M1042: Disable or Remove Feature or Program**)
    - **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.
- 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.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)

- **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-esa-auth-bypass-66kEcxQD

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20798