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:
06/14/2022

SUBJECT:
A Vulnerability in Citrix Application Delivery Management (Citrix ADM) Could Allow for an Unauthenticated Attacker to Reset the Administrator Password

OVERVIEW:
Multiple vulnerabilities have been discovered in Citrix ADM. Citrix ADM is a web-based solution for managing all Citrix deployments. The most severe of these vulnerabilities Could Allow for an Unauthenticated Attacker to Reset the Administrator Password.

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

SYSTEMS AFFECTED:

- Citrix ADM 13.1 before 13.1-21.53
- Citrix ADM 13.0 before 13.0-85.19

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 Citrix ADM. The most severe of these vulnerabilities Could Allow for an Unauthenticated Attacker to Reset the Administrator Password.

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

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

- Corruption of the system by a remote, unauthenticated user. The impact of this can include the reset of the administrator password at the next device reboot, allowing an attacker with ssh access to connect with the default administrator credentials after the device has rebooted. (CVE-2022-27511)
- Temporary disruption of the ADM license service. The impact of this includes preventing new licenses from being issued or renewed by Citrix ADM. (CVE-2022-27512)

Successful exploitation of the most severe of these vulnerabilities can include the reset of the administrator password at the next device reboot, allowing an attacker with ssh access to connect with the default administrator credentials after the device has rebooted.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Citrix once they become available to vulnerable systems immediately after appropriate testing, or **apply an appropriate workaround if an update is not available for your system. Atlassian has recommended to restrict internet access or disabling Confluence Server and Data Center instances**. (https://learn.cisecurity.org/e/799323/ory-2022-06-02-1130377146-html/2db8rw/345956396?h=5RKN7eaMS8GUxlM8X7d5-2PvPhoKVWQ_9fyKl_hnk90) (**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:

Citrix:
https://support.citrix.com/article/CTX460016/citrix-application-delivery-management-security-bulletin-for-cve202227511-and-cve202227512

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27511
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27512