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:
05/19/2022

SUBJECT:
A Vulnerability in VMware Products Could Allow for Authentication Bypass

OVERVIEW:

Multiple vulnerabilities have been discovered in VMware Products, the most severe of which could result in Authentication Bypass.

- VMware Workspace ONE Access is an access control application for Workspace ONE.
- VMware Identity Manager is the identity and access management component of Workspace ONE.
- vRealize Automationi is a management platform for automating the delivery of container-based applications.
- VMware Cloud Foundation is a hybrid cloud platform that provides a set of software-defined services for compute, storage, networking, security and cloud management to run enterprise apps.
- vRealize Suite Lifecycle Manager allows for complete lifecycle and content management capabilities for vRealize Suite products.

Successful exploitation of the most severe of these vulnerabilities could result in Authentication Bypass. A malicious actor may be able to obtain administrative access. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data

THREAT INTELLIGENCE:
CISA anticipates CVE-2022-22972 and CVE-2022-22973 will be exploited in the wild.

SYSTEMS AFFECTED:

- VMware Workspace ONE Access 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0
- VMware Identity Manager 3.3.6, 3.3.5, 3.3.4, 3.3.3

- VMware vRealize Automation 7.6, 8.x
- VMware Cloud Foundation 4.3.x, 4.2.x, 4.1, 4.0.x, 3.x
- vRealize Suite Lifecycle Manager 8.x

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 VMware Products, the most severe of which could result in Authentication Bypass. Details of these vulnerabilities are as follows:

Tactic: *Defense Evasion* **(**TA0005**)**:

Technique: *Modify Authentication Process* **(**T1556**)**:

- A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. (CVE-2022-22972)

Tactic: *Privilege Escalation* **(**TA0029**)**:

Technique: *Abuse Elevation Control Mechanism* **(**T1548**)**:

- A malicious actor with local access can escalate privileges to 'root'.. (CVE-2022-22973)

Successful exploitation of the most severe of these vulnerabilities could result in Authentication Bypass. A malicious actor may be able to obtain administrative access. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by VMware 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.
- 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:

VMware:https://www.vmware.com/security/advisories/VMSA-2022-0014.html

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22972

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22973

CISA:https://www.cisa.gov/emergency-directive-22-03