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:
08/09/2022

SUBJECT:
Multiple Vulnerabilities in VMware vRealize Operations Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in VMware vRealize Operations, the most severe of which could result in Remote Code Execution. VMware vRealize Operations is an IT management platform which enables visibility, optimization and management of an organization's physical, virtual and cloud infrastructure. This software comes within an API which enables developers to build vRealize Operations clients to communicate with the server over HTTP. Successful exploitation of the most severe of these vulnerabilities could allow the attacker to execute code in context of the application. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

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

SYSTEMS AFFECTED:

- VMware vRealize Operations versions prior to 8.6.4

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 vRealize Operations, the most severe of which could result in Remote Code Execution. Details of these vulnerabilities are as follows:

Tactic: *Privilege Escalation* (TA0029), *Execution* (TA0002):

Technique: *Exploitation for Privilege Escalation* (T1404), *Exploitation for Client Execution* (T1203):

- A low-privileged malicious actor with network access can create and leak hex dumps, leading to information disclosure. Successful exploitation can lead to a remote code execution. (CVE-2022-31673)
- An unauthenticated malicious actor with network access may be able to create a user with administrative privileges. (CVE-2022-31675)
- A malicious actor with administrative network access can escalate privileges to root. (CVE-2022-31672)

Details of lower-severity vulnerabilities are as follows:

- A low-privileged malicious actor with network access can access log files that lead to information disclosure. (CVE-2022-31674)

Successful exploitation of the most severe of these vulnerabilities could allow the attacker to execute code in context of the application. 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 patches 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.
    - **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 allowlisting, 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:

VMware:https://www.vmware.com/security/advisories/VMSA-2022-0022.html

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31672

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31673

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31674

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31675