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:

09/22/2021

***09/24/2021* - UPDATED**

SUBJECT:

Multiple Vulnerabilities in VMware vCenter Server Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in VMware vCenter Server, which could result in remote code execution. VMware vCenter Server is a centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts, and all dependent components from a single centralized location. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application.

THREAT INTELLIGENCE:

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

***September 24th* – UPDATED THREAT INTELLIGENCE:**

VMware has reported CVE-2021-22005 is being exploited in the wild. Security researchers are reporting mass scanning for the vulnerability, and publicly available exploit code. CISA expects widespread exploitation of this vulnerability.

SYSTEMS AFFECTED:

- vCenter Server prior to 7.0 Update 2d
- vCenter Server prior to 6.7 Update 3o
- vCenter Server prior to 6.5 Update 3q
- VMware vCloud Foundation prior to version 4.3.1
- VMware vCloud Foundation prior to version 3.10.2.2

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 VMware vCenter Server, which could result in remote code execution. Details of these vulnerabilities are as follows:

- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file. (CVE-2021-22005)
- A malicious actor with non-administrative user access on vCenter Server host may exploit this issue to escalate privileges to Administrator on the vSphere Client (HTML5) or vCenter Server vSphere Web Client (FLEX/Flash). (CVE-2021-21991)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to access restricted endpoints. (CVE-2021-22006)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to perform unauthenticated VM network setting manipulation. (CVE-2021-22011)
- An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance. (CVE-2021-22015)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. (CVE-2021-22012, CVE-2021-22013)
- An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link. (CVE-2021-22016)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to bypass proxy leading to internal endpoints being accessed. (CVE-2021-22017)
- An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts vCenter Server. (CVE-2021-22014)
- A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files. (CVE-2021-22018)
- A malicious actor with non-administrative user access to the vCenter Server vSphere Client (HTML5) and vCenter Server vSphere Web Client (FLEX/Flash) may exploit this issue to create a denial-of-service condition on the vCenter Server host. (CVE-2021-21992)
- An authenticated user with non-administrative privilege may exploit this issue to gain access to sensitive information. (CVE-2021-22007)
- A malicious actor with network access to port 5480 on vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition. (CVE-2021-22019)
- A malicious actor with network access to port 443 on vCenter Server may exploit these issues to create a denial of service condition due to excessive memory consumption by VAPI service. (CVE-2021-22009)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue to create a denial of service condition due to excessive memory consumption by VPXD service. (CVE-2021-22010)
- A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to gain access to sensitive information. (CVE-2021-22008)
- Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server. (CVE-2021-22020)
- An authorized user with access to content library may exploit this issue by sending a POST request to vCenter Server leading to information disclosure. (CVE-2021-21993)

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. A pre-requisite of exploiting these vulnerabilities is that the malicious actor must have network access over port 443 to exploit these vulnerabilities. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by VMware to vulnerable systems immediately after appropriate testing.
- Verify host has not been compromised before applying patches
- Restrict network access to TCP port 443 to authorized hosts or accessible through a VPN
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
VMware:
https://www.vmware.com/security/advisories/VMSA-2021-0020.html
https://via.vmw.com/vmsa-2021-0020-faq

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22020

***September 24th* – UPDATED REFERANCES:**
CISA:
https://us-cert.cisa.gov/ncas/current-activity/2021/09/24/vmware-vcenter-server-vulnerability-cve-2021-22005-under-active

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.