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:
05/26/2021
06/04/2021 ***- UPDATED***

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

OVERVIEW:
Multiple vulnerabilities have been discovered in VMware vCenter Server, the most severe of which could allow for 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 remote code in context of the user running the application.

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

January 23 - UPDATED THREAT INTELLIGENCE:
Threat intelligence firm Bad Packets has reported that hackers are actively scanning the Internet for VMware vCenter servers vulnerable against a critical RCE flaw recently fixed by VMware.

SYSTEMS AFFECTED:

- VMware vCenter Server versions 6.5, 6.7, 7.0

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 remote code execution vulnerability in vCenter Server which enables a malicious actor to execute commands with unrestricted privileges. (CVE-2021-21985)
- An authentication mechanism issue in vCenter Server Plug-ins which enable a malicious actor to perform unauthorized actions. (CVE-2021-21086)

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 be taken:

- Apply appropriate updates provided by VMware to vulnerable systems immediately after appropriate testing.
- 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-2021-0010.html
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21986

June 4th - UPDATED REFERENCES:
Security Affairs:
https://securityaffairs.co/wordpress/118594/hacking/hackers-vmware-vcenter-cve-2021-21985.html?utm_source=feedly&utm_medium=rss&utm_campaign=hackers-vmware-vcenter-cve-2021-21985

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.