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:

03/30/2021

SUBJECT:

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

OVERVIEW:

Multiple vulnerabilities have been discovered in VMware vRealize Operations Manager, which could result in remote code execution. VMware vRealize Operations Manager 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 Manager clients to communicate with the server over HTTP. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application.

THREAT INTELLIGENCE:

These vulnerabilities were reported by Egor Dimitrenko of Positive Technologies which have showcased a successful exploitation attempt utilizing an unrelease proof of concept.

SYSTEMS AFFECTED:

- vRealize Operations Manager Versions 7.5.0, 8.0.0, 8.0.1, 8.1.0, 8.1.1, 8.2.0, 8.3.0

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 vRealize Operations Manager, which could result in remote code execution. Details of these vulnerabilities are as follows:

- A server side request forgery vulnerability in vRealize Operations Manager API which enables a malicious attacker to obtain administrative credentials. (CVE-2021-21975)

- An arbitrary write vulnerability in vRealize Operations Manager API which enable file writes to arbitrary locations within the underlying operating systems. (CVE-2021-21983)

Chaining together both vulnerabilities enables a malicious actor to perform remote code execution in the context of the logged-on user. 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 to the vRealize Operations Manager API.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates provided or workarounds mentioned 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:
Positive Technologies Offensive Team:
https://twitter.com/ptswarm

VMware:
https://www.vmware.com/security/advisories/VMSA-2021-0004.html
https://kb.vmware.com/s/article/83093
https://kb.vmware.com/s/article/83094
https://kb.vmware.com/s/article/83095
https://kb.vmware.com/s/article/83210
https://kb.vmware.com/s/article/83260
https://kb.vmware.com/s/article/82367

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21983

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.