SecurityRisk ADVISORS

CTI Threat Bulletin

VMware vSphere Client and vCenter Server Vulnerabilities

Executive Summary

On May 25th, 2021 VMware released security bulletin VMSA-2021-0010: The bulletin included multiple vulnerabilities in vSphere Client (HTML5), and vCenter Server plugins, the vulnerabilities could allow an unauthenticated attacker to execute code remotely.

Description

A vulnerability has been discovered in the vCenter Server plugin, Virtual SAN Health Check. Through vSphere Client, an adversary can execute code with unrestricted privileges on the host machine if they can access port 443. Please be advised that Virtual San Health check is enabled by default. Another vulnerability has been discovered in a vSphere authentication mechanism for the following plug-ins.

- Virtual San Health Check
- Site Recovery
- vSphere Lifecycle Manager
- VMware Cloud Director Availability

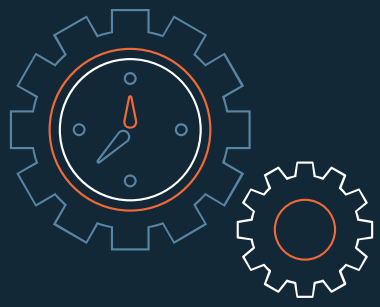
The vulnerability would allow an attacker to perform actions in the plug-ins without authentication.

Affected Products

• vCenter Versions 6.5, 6.7, and 7.0
• Cloud Foundation (vCenter Server) 4.x and 3.x

Safeguards/Recommendations

Affected customers are strongly encouraged to update vCenter to versions 7.0 U2b, 6.7U3n, or 6.5U3p. In addition, Cloud Foundation (vCenter Server), should be updated to 4.2.1 or 3.10.2.1. If any customers are unable to patch right away, the following workaround can implemented for both vulnerabilities. Please see the VMware released security bulletin for more information.



Vendor: VMware

CVE-ID:

CVE-2021-21985,

CVE-2021-21986

Published: May 25, 2021

CVSS V3 Overall score: 9.8, 6.5

Criticality: Critical

Patch Availability: Yes

Vulnerability Type:
Remote Code Execution

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High, Low

Integrity: High, Low

Availability: High, None

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined

References

https://www.vmware.com/security/advisories/VMSA-2021-0010.htm

https://www.vmware.com/security/advisories.html

https://www.zdnet.com/article/patch-immediately-vmware-warns-of-critical-remote-code-execution-holes-in-vcenter/

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io