VMware vCenter Server Critical Vulnerability

VMware vCenter Server remote code execution and authentication vulnerabilities

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

CVEs: CVE-2021-21985 CVE-2021-21986

VMware's virtualization management platform, vCenter Server, has a critical severity bug the company is urging customers to patch "as soon as possible". https://threatpost.com/vmware-ransomware-alarm-critical-bug/166501/ Admins responsible for vCenter machines that have yet to patch CVE-2021-21985 should install the update immediately if possible.

Background

The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Announced

Full details are available from VMWare's announcement at

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

Latest Developments

Threat actors are actively scanning for Internet-exposed & un-patched VMware vCenter servers.

https://www.bleepingcomputer.com/news/security/attackers-are-scanning-for-vulnerable-vmware-servers-patch-now/

Security researchers have also developed and published a proof-of-concept (PoC) RCE exploit code targeting this critical VMware vCenter bug tracked as CVE-2021-21985.

https://www.iswin.org/2021/06/02/Vcenter-Server-CVE-2021-21985-RCE-PAYLOAD/

NMAP script to identify the vulnerability:

https://github.com/alt3kx/CVE-2021-21985_PoC/blob/main/CVE-2021-21985.nse

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*6.0+*	Detects attempts to exploit the vulnerability
	Botnet C&C	*6.0+*	Detects any Botnet C&C activity related to the disclosed IOCs
FortiClient	**Vulnerability**	*6.4+*	Detects VMWare vCenter vulnerabilities (CVE-2021-21985, CVE-2021-21986)
FortiAnalyzer	**Event Handlers & Reports**	*6.2+*	Detects indicators attributed to this vulnerability from Fabric products.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient

Vulnerability
Version Info: 1.246
Link: https://www.fortiguard.com/updates/epvuln?version=1.246

Exploitation

FortiGate

IPS
Version Info: 17.007
Link: https://www.fortiguard.com/updates/ips?version=17.007

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer

Event Handlers & Reports
Version Info: 6.2+
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52767