# **HC3: Sector Alert**

September 22, 2021 TLP: White Report: 202109221409

# VMWare Discloses Numerous Vulnerabilities Posing Active Threat to Healthcare and Public Health (HPH) Sector if Unpatched

#### **Executive Summary**

On September 21, 2021, VMware disclosed numerous vulnerabilities affecting their vCenter Server and Cloud Foundation products, some of which could be exploited for the deployment of ransomware or other malicious activity. Working exploits have already been detected and additional exploits are highly likely to become available soon. VMware recommends that customers install available updates, patches, or workarounds immediately to mitigate these vulnerabilities in affected VMware products.

### Report

On September 21, 2021, VMware disclosed nineteen (19) vulnerabilities affecting their vCenter Server and Cloud Foundation products. Security researchers are particularly concerned about CVE-2021-22005, which was given a CVSSv3 severity rating of 9.8/10 and which could enable a threat actor with network access to port 443 on vCenter Server to upload a malicious file and exploit an unpatched server. Researchers are particularly concerned that this vulnerability (CVE-2021-22005) could be exploited to deploy ransomware on a target organization's network. According to VMware, updates are available to remediate these vulnerabilities in the affected VMware products.

VMWare vCenter Server is the centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts, and all dependent components from a single centralized location. VMware Cloud Foundation provides a complete set of software-defined services for compute, storage, networking, security and cloud management to run enterprise apps—traditional or containerized —in private or public environments.

## **Analysis**

HC3 analysts assess that working exploits are likely being developed for the additional vulnerabilities and it is recommended that organizations implement patches, updates, or workarounds as soon as possible to mitigate risk of exploitation by malicious actors. On September 22, 2021, a security researcher's VMware honeypots detected one instance CVE-2021-22005 exploit activity.

## **Vulnerabilities**

The 19 vulnerabilities—ranging from CVSSv3 4.3 to 9.8—disclosed by VMware on September 22, 2021 for vCenter Server and Cloud Foundation are:

#### **Critical Severity:**

1. CVE-2021-22005 - vCenter Server file upload vulnerability

# **Important Severity:**

- 2. CVE-2021-22018 vCenter Server file deletion vulnerability
- 3. CVE-2021-21992 vCenter Server XML parsing denial-of-service vulnerability
- 4. CVE-2021-22007 vCenter Server local information disclosure vulnerability
- 5. CVE-2021-22019 vCenter Server denial of service vulnerability
- 6. CVE-2021-22009 vCenter Server VAPI multiple denial of service vulnerabilities

# **HC3: Sector Alert**

# September 22, 2021 TLP: White Report: 202109221409

- 7. CVE-2021-22010 vCenter Server VPXD denial of service vulnerability
- 8. CVE-2021-22008 vCenter Server information disclosure vulnerability
- 9. CVE-2021-22020 vCenter Server Analytics service denial-of-service Vulnerability
- 10.CVE-2021-21993 vCenter Server SSRF vulnerability
- 11.CVE-2021-21991 vCenter Server local privilege escalation vulnerability
- 12. CVE-2021-22006 vCenter Server reverse proxy bypass vulnerability
- 13. CVE-2021-22011 vCenter Server unauthenticated API endpoint vulnerability
- 14.CVE-2021-22015 vCenter Server improper permission local privilege escalation vulnerabilities
- 15.CVE-2021-22014 vCenter Server authenticated code execution vulnerability

#### No Severity Level Assigned:

- 16.CVE-2021-22012 vCenter Server unauthenticated API information disclosure vulnerability
- 17.CVE-2021-22013 vCenter Server file path traversal vulnerability
- 18. CVE-2021-22016 vCenter Server reflected XSS vulnerability
- 19. CVE-2021-22017 vCenter Server rhttpproxy bypass vulnerability

## **Patches, Mitigations, and Workarounds**

Updates are available to remediate these vulnerabilities in affected VMware products. Please reference the <u>VMware Security Advisory VMSA-2021-0020</u> for additional information and available workarounds. Additionally, there is a <u>Questions & Answers Blog Post</u> which provided additional guidance and resources.

#### References

VMware. "VMWare Security Advisory VMSA-2021-0020," 21 September 2021. <a href="https://www.vmware.com/security/advisories/VMSA-2021-0020.html">https://www.vmware.com/security/advisories/VMSA-2021-0020.html</a>

VMware. "VMSA-2021-0020: Questions & Answers," 21 September 2021. <a href="https://core.vmware.com/vmsa-2021-0020-questions-answers-fag">https://core.vmware.com/vmsa-2021-0020-questions-answers-fag</a>

Ducket, Chris. "RCE is back: VMware details file upload vulnerability in vCenter Server," 22 September 2021. <a href="https://www.zdnet.com/article/rce-is-back-vmware-details-file-upload-vulnerability-in-vcenter-server/">https://www.zdnet.com/article/rce-is-back-vmware-details-file-upload-vulnerability-in-vcenter-server/</a>

Zorz, Zeljka. "Plug critical VMware vCenter Server flaw before ransomware gangs start exploiting it (CVE-2021-22005)," 22 September 2021. <a href="https://www.helpnetsecurity.com/2021/09/22/cve-2021-22005/">https://www.helpnetsecurity.com/2021/09/22/cve-2021-22005/</a>

Sharwood, Simon. "Break out your emergency change process and patch this ransomware-friendly bug ASAP, says Vmware," 22 September 2021.

https://www.theregister.com/2021/09/22/vmware emergency vcenter patch recommendation/

BadPackets, "Tweet," 22 September 2021.

https://twitter.com/bad\_packets/status/1440739385398362135

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback