TENABLE BLOG

VIEW POSTS BY CATEGORY SEARCH THE BLOG

All

Apply

Subscribe

CVE-2021-22005: Critical File Upload Vulnerability in VMware vCenter Server

Min Read

osure Alerts

an advisory addressing 19
ding one critical flaw in vCenter
tedly simple to exploit.

Background

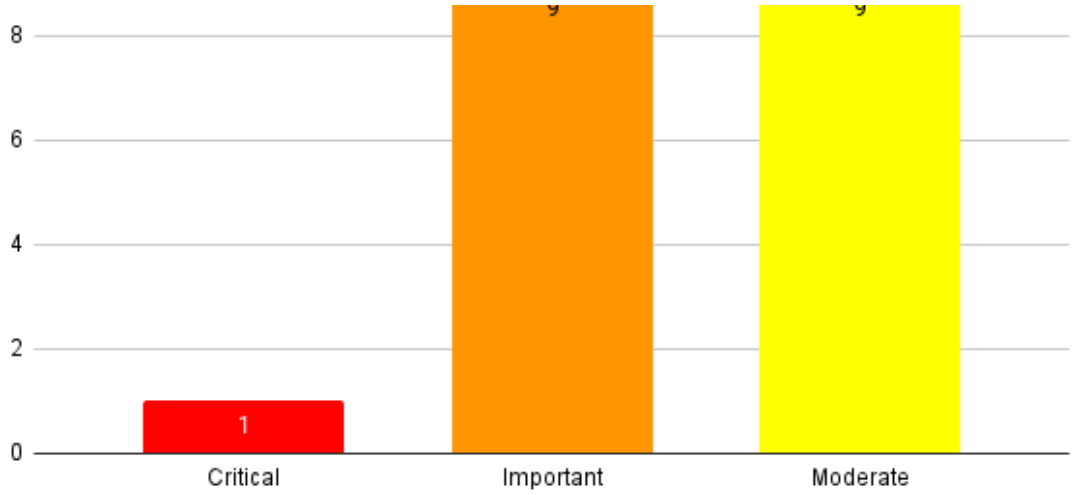
On September 21, VMware published a security advisory addressing 19 vulnerabilities in vCenter Server, its centralized management software for VMware vSphere systems. The full list of vulnerabilities patched includes:

CVE	Description	CVSSv3
CVE-2021-22005	vCenter Server file upload vulnerability	9.8
CVE-2021-21991	vCenter Server local privilege escalation vulnerability	8.8
CVE-2021-22006	vCenter Server reverse proxy bypass vulnerability	8.3
CVE-2021-	er unauthenticated API endpoint vulnerability	8.1
	er improper permission local privilege nerabilities	7.8
	er unauthenticated API information disclosure	7.5
	er file path traversal vulnerability	7.5
	er reflected XSS vulnerability	7.5

22014		
CVE-2021-22018	vCenter Server file deletion vulnerability	6.5
CVE-2021-21992	vCenter Server XML parsing denial-of-service vulnerability	6.5
CVE-2021-22007	vCenter Server local information disclosure vulnerability	5.5
CVE-2021-22019	vCenter Server denial of service vulnerability	5.3
CVE-2021-22009	vCenter Server VAPI multiple denial of service vulnerabilities	5.3
CVE-2021-22010	vCenter Server VPXD denial of service vulnerability	5.3
CVE-2021-22008	vCenter Server information disclosure vulnerability	5.3
CVE-2021-22020	vCenter Server Analytics service denial-of-service Vulnerability	5.0
	er SSRF vulnerability	4.3

021

curity advisory, VMware published a blog post and a
ddressing some foundational questions about the
s, only CVE-2021-22005 was assigned a severity of



Source: Tenable, 2021

Analysis

CVE-2021-22005 is a file upload vulnerability in the vCenter Server. An unauthenticated attacker capable of accessing port 443 over the same network or directly from the internet could exploit a vulnerable vCenter Server by uploading a file to the vCenter Server analytics service. Successful exploitation would result in remote code execution on the host. In its blog post, VMware notes that this vulnerability exists in vCenter Server "regardless of the configuration settings," y default in affected vCenter Server installations.

nerabilities patched in today's release aren't critical, mportant and Moderate severity flaws. The om privilege escalation and denial of service to n traversal vulnerabilities. These flaws will likely be ly affiliates of ransomware groups, that have already gh other means.

ast four months that VMware issued a patch for a Sphere. In May, VMWare disclosed CVE-2021-21985, a ability in VMware's vSphere Client.

o patch as the vulnerability is “trivial to execute”

y officer for Censys, tweeted that he discovered the ulnerability and that it “looks stunningly trivial to dded that users should “Patch now.”

> *It looks stunningly trivial to execute. Patch now.*
>
> *— Derek Abdine (@dabdine) September 22, 2021*

Proof of concept

At the time this blog post was published, there were no publicly available proof-of-concept (PoC) scripts for CVE-2021-22005. However, Abdine's warning implies that we may see PoC released shortly.

Solution

To address the 19 vulnerabilities disclosed in its advisory, VMware released patches for vCenter Server 7.0, 6.7 and 6.5. For a full breakdown of which CVEs are addressed in each release, please refer to the VMware advisory page.

For CVE-2021-22005, the following is a breakdown of the vCenter Server version, associated fixed version as well as the installation addressed.

Version of vCenter Server	Fixed Version	Installation
7.0	7.0 U2c	Any
	6.7 U3o	Virtual Appliance

er version 6.7 for Windows and version 6.5 for any
CVE-2021-22005.

ouraged to apply these patches as soon as possible.

s time, VMware has provided workaround instructions
the workaround should be considered a temporary
placement for upgrading to a fixed version.

ected systems

Get more information

VMware Advisory VMSA-2021-0020

VMware VMSA-2021-0020 Blog Post: What You Need To Know

VMware VMSA-2021-0020: Questions & Answers

VMware Workaround Instructions for CVE-2021-22005

Join Tenable's Security Response Team on the Tenable Community.

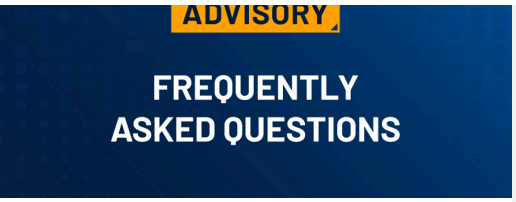
Learn more about Tenable, the first Cyber Exposure platform for holistic management of your modern attack surface.

Get a free 30-day trial of Tenable.io Vulnerability Management.

Satnam Narang

Satnam joined Tenable in 2018. He has over 15 years experience in the industry (M86 Security and Symantec). He contributed to the Anti-Phishing Working Group, helped develop a Social Networking Guide for the National Cyber Security Alliance, uncovered a huge n Twitter and was the first to report on spam bots appeared on NBC Nightly News, Entertainment nberg West, and the Why Oh Why podcast.

ide of work: Satnam writes poetry and makes hip- enjoys live music, spending time with his ootball and basketball, Bollywood movies and music by Yoda).



CVE-2024-47575: Frequently Asked Questions About FortiJump Zero-Day in FortiManager and FortiManager Cloud

October 23, 2024

Frequently asked questions about a zero-day vulnerability in Fortinet's FortiManager that has reportedly been exploited

From Bugs to Breaches: 25 Significant CVEs As MITRE CVE Turns 25

October 22, 2024

Twenty five years after the launch of CVE, the Tenable Security Response Team has handpicked 25 vulnerabilities that stand out for their significance.

Tenable Security Response Team

Oracle October 2024 Critical Patch Update Addresses 198 CVEs

October 15, 2024

Oracle addresses 198 CVEs in its fourth quarterly update of 2024 with 334 patches, including 35 critical updates.

Tenable Security Response Team

from the experts at Tenable.

Featured products

Tenable One Exposure Management Platform

Tenable Cloud Security

Tenable CIEM

Tenable Vulnerability Management

Tenable Web App Scanning

Tenable Enclave Security

Tenable Attack Surface Management

Tenable Identity Exposure

General manufacturing
Generative AI
Healthcare
Hybrid cloud security
IT/OT
Ransomware
State / Local / Education
US federal
Vulnerability management
Zero trust
View all ›

Customer resources
Resource library
Community & support
Customer education
Tenable Research