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

September 22, 2021 • 5 Min Read
by Satnam Narang
Blog Home / Cyber Exposure Alerts

VMware published an advisory addressing 19 vulnerabilities, including one critical flaw in vCenter Server that is reportedly simple to exploit.

Background

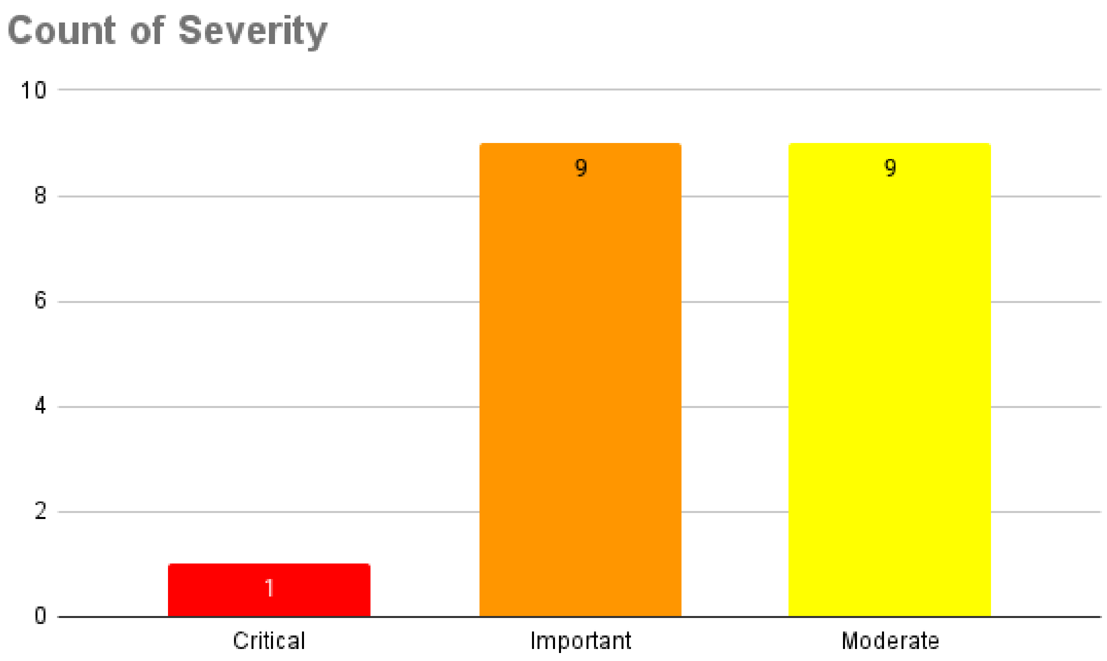
On September 21, VMware published a security advisory addressing 19 vulnerabilities in vCenter Server, its centralized management software for VMware vSphere systems. The full list of vulnerabilities patched includes:

CVE	Description	CVSSv3
	r Server file upload vulnerability	9.8
	r Server local privilege escalation vulnerability	8.8
	r Server reverse proxy bypass vulnerability	8.3
	r server unauthenticated API endpoint vulnerability	8.1
	r Server improper permission local privilege escalation vulnerabilities	7.8
	r Server unauthenticated API information disclosure vulnerability	7.5

CVE-2021-22017	vCenter Server rhttpproxy bypass vulnerability	7.3
CVE-2021-22014	vCenter Server authenticated code execution vulnerability	7.2
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
CVE-2021-21993	vCenter Server SSRF vulnerability	4.3

Source: VMware, September 2021

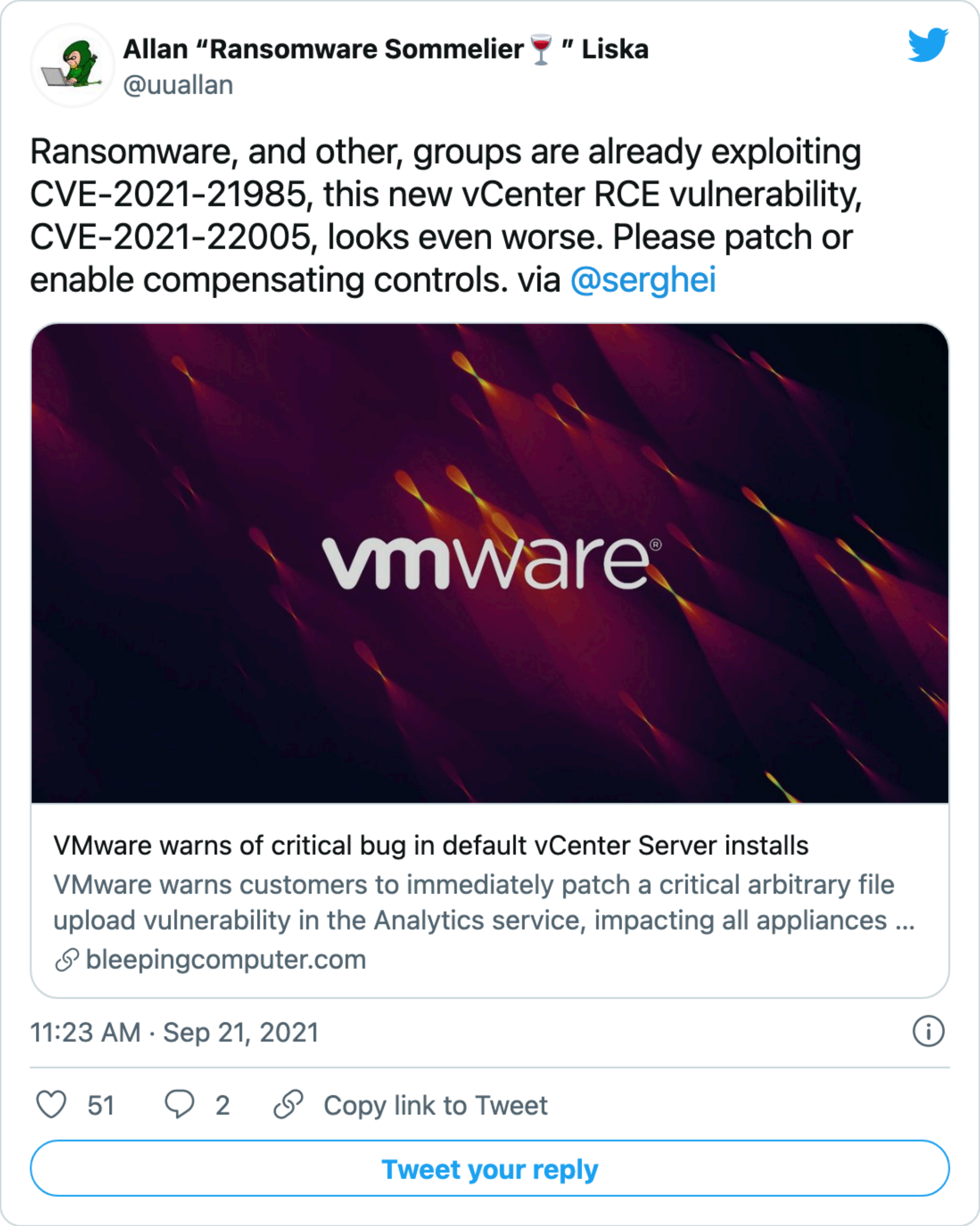
In addition to publishing the security advisory, VMware published a blog post and a Questions and Answers post addressing some foundational questions about the advisory. Of the 19 vulnerabilities, only CVE-2021-22005 was assigned a severity of Critical.



Source: Tenable, 2021

d vulnerability in the vCenter Server. An unauthenticated attacker capable of ame network or directly from the internet could exploit a vulnerable vCenter Server ter Server analytics service. Successful exploitation would result in remote code log post, VMware notes that this vulnerability exists in vCenter Server "regardless of hich makes this exploitable by default in affected vCenter Server installations.

lnerabilities patched in today's release aren't critical, they are split evenly between rity flaws. The remaining vulnerabilities vary, from privilege escalation and denial of ure and path traversal vulnerabilities. These flaws will likely be valuable to attackers, Security researcher Allan Liska tweeted that CVE-2021-21985 has already been leveraged as part of ransomware attacks and that CVE-2021-22005 "looks even worse."



Allan "Ransomware Sommelier 🍷 " Liska
@uuallan

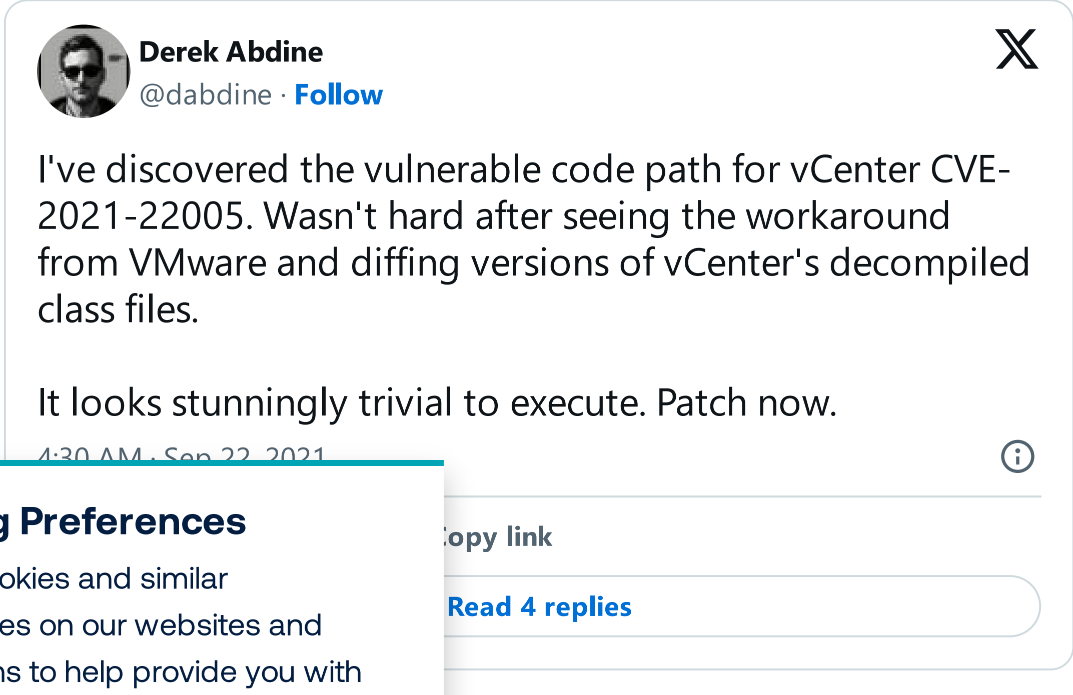
Ransomware, and other, groups are already exploiting CVE-2021-21985, this new vCenter RCE vulnerability, CVE-2021-22005, looks even worse. Please patch or enable compensating controls. via @serghei

VMware warns of critical bug in default vCenter Server installs
VMware warns customers to immediately patch a critical arbitrary file upload vulnerability in the Analytics service, impacting all appliances ...
bleepingcomputer.com

11:23 AM · Sep 21, 2021

Researchers stress urgency to patch as the vulnerability is "trivial to execute"

Derek Abdine, chief technology officer for Censys, tweeted that he discovered the vulnerable code path for this vulnerability and that it "looks stunningly trivial to execute." As a result, Abdine added that users should "Patch now."



Derek Abdine
@dabdine · Follow

I've discovered the vulnerable code path for vCenter CVE-2021-22005. Wasn't hard after seeing the workaround from VMware and diffing versions of vCenter's decompiled class files.

It looks stunningly trivial to execute. Patch now.

4:30 AM · Sep 22, 2021

ept

published, there were no publicly available proof-of-concept (PoC) scripts for CVE-'s warning implies that we may see PoC released shortly.

as the installation addressed.

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

Please note that vCenter Server version 6.7 for Windows and version 6.5 for any installation are not affected by CVE-2021-22005.

Organizations are strongly encouraged to apply these patches as soon as possible.

If patching is not feasible at this time, VMware has provided workaround instructions for CVE-2021-22005. However, the workaround should be considered a temporary solution and should not be a replacement for upgrading to a fixed version.

Identifying affected systems

A list of Tenable plugins to identify these vulnerabilities will appear here as they're released.

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.

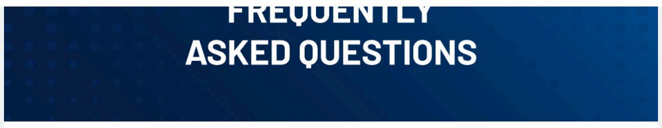
Get a free 30-day trial of Tenable.io Vulnerability Management.

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 spam botnet on Twitter and was the first to report on spam bots on Tinder. He's appeared on NBC Nightly News, Entertainment Tonight, Bloomberg West, and the Why Oh Why podcast.

s outside of work: Satnam writes poetry and makes hip-hop music. He enjoys live
pending time with his three nieces, football and basketball, Bollywood movies and
d Grogu (Baby Yoda).

RELATED ARTICLES



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 in the wild.

By Satnam Narang , Rody Quinlan , and Scott Caveza

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

CYBERSECURITY NEWS YOU CAN USE

Enter your email and never miss timely alerts and security guidance from the experts at Tenable.

email@example.com

Submit

tenable

Tracking Preferences

We use cookies and similar technologies on our websites and applications to help provide you with the best possible online experience. By selecting "Opt in" below, you agree that we may store and access cookies and similar technologies on your device. Read more in our privacy policy.

ured solutions

e Directory
ng management
ms
l security posture
agement
pliance
sure management

Customer resources

Resource library
Community & support
Customer education
Tenable Research
Documentation
Nessus resource center

Connections

Blog
Contact us
Careers
Investors
Tenable Ventures
Events

Tenable OT Security
Tenable Security Center
Tenable Lumin
Tenable Nessus

View all ›

Hybrid cloud security
IT/OT
Ransomware
State / Local / Education
US federal
Vulnerability management
Zero trust

View all ›

Privacy policy | Do not sell/share my personal information | Legal | 508 compliance