H E A D Q U A R T E R S
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

Wide Exploitation of New VMware vCenter Server Flaw Likely

Organizations using VMware's vCenter Server that haven't yet applied a patch for a recently disclosed arbitrary file upload vulnerability in the management utility (CVE-2021-22005) are at heightened risk of compromise.

The US Cybersecurity & Infrastructure Security Agency (CISA) on Friday warned organizations to expect "widespread exploitation" of the flaw because of publicly available exploit code. The advisory noted a Sept. 24 confirmation by VMware of CVE-2021-22005 being actively exploited in the wild.

The CISA advisory also pointed to reports by security researchers of mass scanning activity for vulnerable vCenter Servers by threat actors. The agency strongly urged critical infrastructure entities and other users with affected versions of the technology to apply VMware's patch for the flaw as "quickly as possible." Organizations that are unable to immediately upgrade to a fixed version of the technology should consider implementing VMware's workaround instructions for CVE-2021-22005, CISA said.

VMware's vCenter Server is a utility that allows administrators to centrally manage vSphere virtual machine infrastructure. VMware describes it as technology that organizations can use to manage the security and availability of vSphere environments, to simplify tasks, and to reduce some of the complexity involved in managing virtual environments.

Déjà Vu

This marks the second time in recent months that organizations using vCenter Servers have been forced to scramble to address critical vulnerabilities in the technology. In June, CISA issued a similar warning involving another critical remote code execution flaw (CVE-2021- 21985). VMware issued a patch for that issue in May, but even weeks later, thousands of vulnerable systems remained unpatched, prompting CISA to issue the alert. At the time, CISA warned about unpatched systems remaining an attractive target for attackers and giving threat actors a way to take complete controls of vulnerable systems.

The newly disclosed CVE-2021-22005 arbitrary file upload vulnerability is the most critical among a set of 19 unique vulnerabilities that multiple security researchers privately reported to VMware recently. Any attacker that can reach vCenter Server over the network can gain access to it regardless of the server's configuration settings, VMware warned.

VMware has assigned the flaw a severity rating of 9.8, which makes it a highly critical vulnerability on the 10-point CVSSv3 vulnerability rating scale. "A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file," VMware said. The affected versions of the software are vCenter Server versions 6.5, 6.7, and 7.0 and VMware Cloud Foundation.

Alec Alvarado, threat intelligence team lead at Digital Shadows, says that certain details of the publicly available proof of concept (PoC) have purposefully been left out so that threat actors cannot easily carry out the remote code execution component of the attack. However, technically sophisticated attackers can likely figure it out, he says.

"Threat actors follow the news just as much as security researchers, quite possibly more," Alvarado says. "With a nearly functional PoC out there, technically sophisticated [threat actors] interested in leveraging the vulnerability already are leveraging it." When a complete PoC is published, expect less sophisticated actors to start targeting the flaw, Alvarado notes.

VMware urged organizations to immediately apply the patch it issued last week for the flaw. "These updates fix a critical security vulnerability, and your response needs to be considered at once," the company said.

Workaround Measures

For organizations that cannot immediately update their software to the patched version, VMware has released specific workaround measures. Administrators can implement the workaround using a script that VMware has developed for vulnerable vCenter servers. Or they can implement the workaround manually by following steps the company has released for doing it. VMware warned organizations to consider the workaround as a temporary measure until the update can be applied.

John Bambenek, principal threat hunter at Netenrich, says that any flaw that enables remote code execution with root-level privileges on virtual machines is significant. "Nearly every business operates virtual machines," he says, "and if I have root access, I could ransom every machine in that environment or steal the data on those virtual machines with relative ease."

References:

https://thehackposts.com/wide-exploitation-of-new-vmware-vcenter-server-flaw-likely/

https://www.itsecuritynews.info/cisa-wide-exploitation-of-new-vmware-vcenter-server-flaw-likely/

https://aeternusmalus.wordpress.com/2021/09/27/cisa-wide-exploitation-of-new-vmware-vcenter-server-flaw-likely/

https://www.securityweek.com/vmware-calls-attention-high-severity-vcenter-server-flaw