MUST READ: Want to create a successful data strategy? Here's where you need to start

Patch immediately: VMware warns of critical remote code execution hole in vCenter

If an attacker hits port 443, they could execute whatever code they please on the host operating system thanks to a vulnerability in vCenter.

By Chris Duckett | May 26, 2021 -- 01:15 GMT (18:15 PDT) | Topic: Security

Image: MaboHH / Getty Images

VMware is urging its vCenter users to update vCenter Server versions 6.5, 6.7, and 7.0 immediately, after a pair of vulnerabilities were reported privately to the company.

The most pressing is CVE-2021-21985, which relates to a remote code execution vulnerability in a vSAN plugin enabled by default in vCenter that an attacker could use to run whatever they wished on the underlying host machine, provided they can access port 443.

Even if users do not use vSAN, they are likely to be affected because the vSAN plugin is enabled by default.

"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 described the issue in an advisory (https://www.vmware.com/security/advisories/VMSA-2021-0010.html).

In its FAQ (https://core.vmware.com/resource/vmsa-2021-0010-faq), VMware warned that since the attacker only needs to be able to hit port 443 to conduct the attack, firewall controls are the last line of defence for users.

"Organisations who have placed their vCenter Servers on networks that are directly accessible from the internet may not have that line of defence and should audit their systems for compromise," the company states.

"They should also take steps to implement more perimeter security controls (firewalls, ACLs, e gement interfaces of their infrastructure."

To fix the issue, VMware recommends users update vCenter, or if not possible, the company has provided instructions (https://kb.vmware.com/s/article/83829) on how to disable vCenter Server plugins.

"While vSAN will continue operating, manageability and monitoring are not possible while the plugin is disabled. A customer who is using vSAN should only consider disabling the plugin for short periods of time, if at all," VMware warned.

Users are warned that the patches provide better plugin authentication, and some third-party plugins may break and users are directed to contact the plugin vendor.

"This needs your immediate attention if you are using vCenter Server," VMware said in a blog post (https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html).

"In this era of ransomware it is safest to assume that an attacker is already inside the network s desktop and perhaps even in control of a user account, which is why we

strongly recommend declaring an emergency change and patching as soon as possible."

Even having perimeter controls may not be enough, and VMware suggested users look at better network separation.

"Ransomware gangs have repeatedly demonstrated to the world that they are able to compromise corporate networks while remaining extremely patient, waiting for a new vulnerability in order to attack from inside a network," it said.

"This is not unique to VMware products, but it does inform our suggestions here. Organisations may want to consider additional security controls and isolation between their IT infrastructure and other corporate networks as part of an effort to implement modern zero-trust security strategies."

The second vulnerability, CVE-2021-21986, would allow an attacker to perform actions allowed by plugins without authentication.

"The vSphere Client (HTML5) contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins," VMware said.

In terms of CVSSv3 scores, CVE-2021-21985 hit an 9.8, while CVE-2021-21986 was scored as 6.5.

Earlier this year, a pair of ESXi vulnerabilities (https://www.zdnet.com/article/ransomware-gangs-are-abusing-vmware-esxi-exploits-to-encrypt-virtual-hard-disks/) were being used ransomware gangs to take over virtual machines and encrypt virtual hard drives.

RELATED COVERAGE

- Dell divests VMware: Investors cheer, but what does it mean for customers? (/article/dell-divests-vmware-investors-cheer-but-what-does-it-mean-for-customers/)
- VMware patches critical vRealize Operations platform vulnerabilities (/article/vmware-patches-critical-vrealize-operations-vulnerabilities/)
- More than 6,700 VMware servers exposed online and vulnerable to major new bug (/article/more-than-6700-vmware-servers-exposed-online-and-vulnerable-to-major-new-bug/)
- Ransomware gangs are abusing VMWare ESXi exploits to encrypt virtual hard disks (/article/ransomware-gangs-are-abusing-vmware-esxi-exploits-to-encrypt-virtual-hard-disks/)
- VMware's blockchain platform is ready for the enterprise (/article/vmwares-blockchain-platform-is-ready-for-the-enterprise/)

RELATED TOPICS: VIRTUALIZATION SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Chris Duckett | May 26, 2021 -- 01:15 GMT (18:15 PDT) | Topic: Security

SHOW COMMENTS

Manage Cookies