VMware warns of critical bug in default vCenter Server installs

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 21, 2021 01:40 PM **0**

VMware warns customers to immediately patch a critical arbitrary file upload vulnerability in the Analytics service, impacting all appliances running default vCenter Server 6.7 and 7.0 deployments.

vCenter Server (https://www.vmware.com/products/vcenter-server.html) is a server management solution that helps IT admins manage virtualized hosts and virtual machines in enterprise environments via a single console.

"In this era of ransomware it is safest to assume that an attacker is already inside your network somewhere, on a 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*."

Critical bug with an almost perfect severity score

The security flaw — tracked as **CVE-2021-22005 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22005)** and with a CVSS 3.1 severity rating of 9.8/10 (https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) — can be exploited by attackers to execute commands and software on unpatched vCenter Server deployments by uploading a specially crafted file.

This bug was reported by George Noseevich and Sergey Gerasimov of SolidLab LLC, and it can be exploited by unauthenticated attackers remotely in low complexity attacks that don't require user interaction.

"The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service," VMware explains in the security advisory (https://www.vmware.com/security/advisories/VMSA-2021-0020.html). "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."

According to the company, patching this vulnerability should be added to the top of any IT admin's task list, given that working exploits will likely surface right after the bug's disclosure.

"With the threat of ransomware looming nowadays the safest stance is to assume that an attacker may already have control of a desktop and a user account through the use of techniques like phishing or spearphishing, and act accordingly.

"This means the attacker may already be able to reach vCenter Server from inside a corporate firewall, and time is of the essence."

Workaround also available

VMware also provides a workaround for those who cannot immediately patch their appliances as a temporary solution.

The steps detailed here (https://kb.vmware.com/s/article/85717) require you to edit a text file on the virtual appliance and restarting services manually or using a VMware-provided script to remove the possibility of exploitation.

A detailed FAQ document with additional questions and answers regarding the CVE-2021-22005 vulnerability is available here (https://core.vmware.com/vmsa-2021-0020-questions-answers-faq).

In May, VMware issued a similar warning regarding a critical remote code execution (RCE) flaw (https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-bug-affecting-all-vcenter-server-installs/) in the Virtual SAN Health Check plug-in impacting all vCenter Server deployments.

Another critical RCE bug affecting all vCenter Server deployments (https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/) running a vulnerable vCenter Server plug-in for vRealize Operations (vROps) present in all default installations was fixed in February.