Code-execution flaw in VMware has a severity rating of 9.8 out of 10

By Dan Goodin

Published: 2021-02-25 · Archived: 2026-04-06 03:31:39 UTC

Hackers are mass-scanning the Internet in search of VMware servers with a newly disclosed code-execution vulnerability that has a severity rating of 9.8 out of a possible 10.

CVE-2021-21972, as the security flaw is tracked, is a remote code-execution vulnerability in VMware vCenter server, an application for Windows or Linux that administrators use to enable and manage virtualization of large networks. Within a day of VMware issuing a patch, proof-of-concept exploits appeared from at least six different sources. The severity of the vulnerability, combined with the availability of working exploits for both Windows and Linux machines, sent hackers scrambling to actively find vulnerable servers.

“We’ve detected mass scanning activity targeting vulnerable VMware vCenter servers (https://vmware.com/security/advisories/VMSA-2021-0002.html),” researcher Troy Mursch of Bad Packets wrote.

Mursch said that the BinaryEdge search engine found almost 15,000 vCenter servers exposed to the Internet, while Shodan searches revealed about 6,700. The mass scanning is aiming to identify servers that have not yet installed the patch, which VMware released on Tuesday.

Unfettered code execution, no authorization required

CVE-2021-21972 allows hacker with no authorization to upload files to vulnerable vCenter servers that are publicly accessible over port 443, researchers from security firm Tenable said. Successful exploits will result in hackers gaining unfettered remote code-execution privileges in the underlying operating system. The vulnerability stems from a lack of authentication in the vRealize Operations plugin, which is installed by default.

The flaw has received a severity score of 9.8 out of 10.0 on the Common Vulnerability Scoring System Version 3.0. Mikhail Klyuchnikov, the Positive Technologies researcher who discovered the vulnerability and privately reported it to VMware, compared the risk posed by CVE-2021-21972 to that of CVE-2019-19781, a critical vulnerability in the Citrix Application Delivery Controller.

Source: https://arstechnica.com/information-technology/2021/02/armed-with-exploits-hackers-on-the-prowl-for-a-critical-vmware-vulnerability/