



VULNERABILITY BULLETINS

Multiple Vulnerabilities in VMware vSphere Client (HTML5)



TLP:WHITE

Jun 07, 2021

On June 4, 2021, Cybersecurity and Infrastructure Security Agency (CISA) published an alert, [Unpatched VMware vCenter Software](#), related to the likelihood that cyber threat actors are attempting to exploit CVE-2021-21985, a remote code execution vulnerability in VMware vCenter Server and VMware Cloud Foundation.

Although patches were made [available](#) on May 25, 2021, unpatched systems remain an attractive target and attackers can exploit this vulnerability to take control of an unpatched system. VMware vCenter Server and VMware Cloud Foundation are part of the underlying infrastructure for most organizations with on-premises network management.

Reference(s)

[VMware](#), [CISA](#), [VMware](#), [VMware](#), [VMware](#)

CVE(s)

CVE-2021-21985

Recommendations

CISA encourages state and local governments, critical infrastructure entities, including healthcare, and other private sector organizations to review VMSA-21-0010, [blogpost](#), and [FAQ](#) for more information about the vulnerability and apply the necessary updates as soon as possible, even if out-of-cycle work is required.

If your organization cannot immediately apply the update, then apply the [workarounds](#) in the interim.

Sources

<https://www.vmware.com/security/advisories/VMSA-2021-0010.html>

<https://www.vmware.com/security/advisories/VMSA-2021-0010.html>

<https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html>

<https://core.vmware.com/resource/vmsa-2021-0010-faq>

<https://kb.vmware.com/s/article/83829>

Alert ID eaa2a133

[View Alert](#)

Tags CVE-2021-21985, CISA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.