HHS Office for Civil Rights in Action

Cyber Alert: Updates on Ransomware and Critical VMware Vulnerability

OCR is sharing the following alerts from the White House and Cybersecurity and Infrastructure Security Agency (CISA). Organizations are encouraged to review the information below and take appropriate action.

White House Memo: What We Urge You To Do To Protect Against The Threat of Ransomware

Anne Neuberger the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology has released a memo titled "What We Urge You To Do To Protect Against The Threat of Ransomware." This memo addresses the growing number and size of ransomware incidents and calls upon government and private sector to take steps to protect their organizations from this growing threat. The memo also outlines the U.S. Government's recommended best practices – a small number of highly impactful steps to help your organization focus and make rapid progress on driving down risk.

Below are a variety of resources that you can use to keep your healthcare facility protected from ransomware attacks:

- CISA Ransomware Guidance and Resources
- CISA Ransomware Guide
- DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
- FBI Ransomware Webpage
- FBI IC3 Webpage for Ransomware
- NIST's Tips and Tactics for Dealing with Ransomware
- HHS HC3 Homepage
- 405(d) Ransomware Threat Flyer
- 405(d) Spotlight Webinar- Ransomware
- 405(d) Ransomware Cyber Awareness Flyer
- Ransomware Task Force: Combatting Ransomware Report
- Software Engineering Institute Resources for Preparing and Responding to Ransomware

In addition to these materials, the HHS Office for Civil Rights' Fact Sheet: Ransomware and HIPAA provides further information for entities regulated by the HIPAA Rules.

CISA Alert on Critical VMware Vulnerability - PATCH IMMEDIATELY IF FOUND

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of 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. This vulnerability was discussed on the May 27 CISA weekly Security Operation Centers (SOC) call.

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 agencies with on premises network management. Based off CISA visibility, several agencies are showing unpatched instances of these products.

CISA encourages agencies, state and local governments, critical infrastructure entities, and other private sector organizations to review VMware's 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.

Notification Links:

- 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

To report an incident or indicators of potential compromise, visit https://us-cert.cisa.gov/report.