American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

June 16, 2023

MOVEit Transfer Vulnerability Strikes – Here's What Hospitals and Health Systems Must Know About the New Ransomware Risk

With multiple hospitals and federal agencies victimized by emerging Russia-linked cyberthreat, hospitals must take immediate steps to harden their defenses

A Russia-linked ransomware gang is exploiting a security flaw in MOVEit Transfer, a tool used by hospitals, health systems, corporations and government agencies to share large files over the internet, resulting in a serious ransomware threat against critical infrastructure. The privilege escalation vulnerability is being employed by the CLOP ransomware gang to infiltrate organizations' systems; in an unusual step, CLOP is not contacting its victims to demand payment, but instead posted a blackmail message posted on its dark web leak site.

Due to the scope and scale of organizations targeted, including government agencies, this strategic cyberthreat may be related to ongoing geopolitical tensions with Russia. Based upon previous methodology and public information regarding Russian cyber gangs, this group may be operating with the tacit or explicit approval of the Russian intelligence services.

The CLOP gang is also attributed to cyberattacks using "zero day" vulnerabilities targeting the GoAnywhere MFT platform and the Accellion File Transfer Appliance.

Hospitals and health systems are urged to take the following, immediate steps:

- Identify any presence of the MOVEit Transfer application in your network.
- Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment.
- Take action to apply the patch developed to address the June 15 CVE-2023-35708 vulnerability discovered in MOVEit Transfer.
- Review the MOVEit Transfer advisory, follow the mitigation steps, and apply the necessary updates when available, along with the joint FBI/CISA alert.
- Identify other secure file transfer applications, assess their necessity and access, and ensure they are fully patched.
- Share this AHA Cybersecurity Advisory with your organization's IT and cyber infrastructure teams.
- Review the above-identified alerts and bulletins for guidance on risk mitigation procedures, including increased network monitoring for unusual network traffic or activity, especially around active directories. Additionally, it is important to heighten staffs' awareness of increased risk of receiving phishing emails.

- Install updates for operating systems, software and firmware as soon as they are released.
- If you use Remote Desktop Protocol (RDP), or other potentially risky services, secure and monitor them closely. Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity. Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established protocol. Open document readers in protected viewing modes to help prevent active content from running.
- Implement user training programs and phishing awareness exercises that increase users' understanding about the risks of visiting suspicious websites, clicking on suspicious links and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- Require phishing-resistant MFA for as many services as possible, particularly for webmail, VPNs, accounts that access critical systems and privileged accounts that manage backups.
- Use strong passwords and avoid reusing passwords for multiple accounts.
- Require administrator credentials to install software.
- Audit user accounts with administrative or elevated privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Only use secure networks and avoid using public wi-fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.