Healthcare Law Alert: CISA, FBI and OCR Cyber Alerts Concerning Ransomware Attacks and Systems Vulnerabilities

7/14/2021

Kaseya Vulnerability and Ransomware Attacks

The Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA) have released guidance in response to the recent supply-chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs) and their customers. The Kaseya RMM tool is widely used in the healthcare sector. CISA and FBI strongly urge affected MSPs and their customers to follow the guidance and also review the Kaseya Important Notice published on July 9, 2021. On July 12, 2021, CISA issued another notice, regarding security updates for VSA on-premises software vulnerabilities, and on July 14, 2021, issued a further Important Notice. The Department of Health & Human Services, Office for Civil Rights (OCR) also has distributed information concerning these attacks and the guidance to its listserv. Healthcare providers should continue to look for updates and notices relating to these vulnerabilities and attacks.

Kaseya warns that:

Spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments or phones claiming to be Kaseya Partners – DO NOT click on links or download attachments and DO NOT respond to phone calls claiming to be a Kaseya Partner.

Among other things, CISA and FBI recommend that affected MSPs:

- Contact Kaseya at support@kaseya.com with the subject “Compromise Detection Tool Request” to obtain and run Kaseya’s Compromise Detection Tool available to Kaseya VSA customers. The tool is designed to help MSPs assess the status of their systems and their customers’ systems;
- Enable and enforce multi-factor authentication (MFA) on every single account that is under the control of the organization, and—to the maximum extent possible—enable and enforce MFA for customer-facing services;
- Implement allow listing to limit communication with remote monitoring and management (RMM) capabilities to known IP address pairs; and/or
- Place administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.

Affected MSP customers should ensure backups are up to date and stored in an easily retrievable location that is air-gapped from the organizational network. Further technical assistance can be found here.

Security Advisory for Philips Vue PAC Products

On July 6, 2021, CISA released a Security Advisory for Philips View PAC Products, including ICS Medical Advisory (ICSMA-21-187-01), detailing vulnerabilities in multiple Philips Clinical Collaboration Platform Portal (officially registered as Vue PACS) products. Per the advisory, an attacker could exploit some of these vulnerabilities and take control of an affected system. Users and administrators are encouraged to review the ICS Medical Advisory and to apply the necessary updates or workarounds.

Important Reminder

These latest attacks and alerts serve as reminders that healthcare providers must ensure they have in place a robust and active HIPAA/data privacy and security program, including policies and procedures, training, oversight, periodic risk assessments to detect risks and vulnerabilities to systems and protected health information, and risk management plans to address identified risks and vulnerabilities.

For additional information or assistance, contact:

Lani M. Dornfeld, CHPC, Member, Healthcare Law, at 973-403-3136 or ldornfeld@bracheichler.com

John D. Fanburg, Managing Member and Chair, Healthcare Law, at 973-403-3107 or jfanburg@bracheichler.com

Joseph M. Gorrell, Member, Healthcare Law, at 973-403-3112 or jgorrell@bracheichler.com

Carol Grelecki, Member, Healthcare Law, at 973-403-3140 or cgrelecki@bracheichler.com