Kaseya VSA Supply Chain Ransomware Attack

HHS 405(d) Program SBAR Brief

July 28, 2021

The 405(d) **S**ituation, **B**ackground, **A**ssessment, **R**ecommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the Cybersecurity Act of 2015 with the goal of aligning industry security approaches, the 405(d) **SBARs**, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: Kaseya, an IT software company suffered a supply chain ransomware attack on July 2, 2021. Many small to medium sized businesses were affected due to ransomware deployed onto Managed Service Provider's (MSP's) customers' computers. Managed Service Provider's (MSP) provide active administrative support for application, infrastructure and network security. On-going hosting support is provided to customers on -site or in a third-party data center. Customers' data were encrypted and held for ransom due to the supply chain attack. It is not known at this time how many organizations have been affected. However, it is estimated that this attack will affect hundreds of companies that utilize the Kaseya Virtual System/Server Administrator (VSA) product. Kaseya's CEO stated in an interview that "between 50-60 of the company's 37,000 customers were compromised. But 70% were managed service providers who use the company's hacked VSA software to manage multiple customers."[1]

Pertinent and brief information related to the situation

BACKGROUND: The MSP's used the Kaseya Virtual System/Server Administrator (VSA) product to assist them with managing their small to medium sized customer's IT infrastructure. In most situation's small to medium healthcare offices do not have an internal dedicated IT department. Therefore organizations can leverage the expertise of MSPs to assist with IT issues such as patching, backups, and maintaining multiple servers. Although MSP's provide useful infrastructure solutions; their software can be compromised which creates many vulnerabilities for small medical organizations. Vulnerabilities such as supply chain ransomware attacks can leave facilities without access to patient data or access to medical devices for days or even months.

Analysis and considerations of options—what we found and think

ASSESSMENT: A supply chain attack is an attack where a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers."[2] The software comes from trusted sources which reduces the likelihood of anti-virus software detecting its presence in the network. Supply Chain attacks cause a ripple effect because of the process in which the software is disseminated onto the end users' computer. The software company that creates the product is affected and so is the company that provides the software to the small business.

These types of attacks are becoming more common in the healthcare industry due to outsourced IT services. MSP software can provide malware with elevated network access and privileges which hackers can exploit and encrypt data for ransom. This is increasingly volatile in the healthcare industry where medical devices are utilized to monitor patient's vital signs and store sensitive Protected Health Information (PHI).

Recommended/ requested action—what we want you to do

RECOMMENDATION: MSPs provide a large selection of infrastructure services ranging from application security to network monitoring. They provide ongoing support to healthcare organizations and keep their environment secure. These services are offered on a contractual basis to the customer's premises. It is important to remember that although the MSPs manage the network on behalf of the organization, systems are always vulnerable to breaches. Therefore, it is imperative that your organization implements proper measures to back-up data and implement a disaster recovery plan.

Another recommendation that will assist with minimizing the impact of the ransomware attack, is to run an intrusion detection tool on your network. Kaseya has provided a free of charge VSA Detection Tool that is available to everyone. The tool is designed to "analyze a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IOCs) are present."[2]

It is highly recommended that every organization that is utilizing Kaseya Services run the Kaseya VSA Detection tool on their network to determine if they have been affected. This will help with discovering any vulnerabilities that were caused from the ransomware attack. Therefore, enabling your organization to begin the disaster recovery process. Even if you are not currently utilizing the Kaseya products, it is recommended to install and run the tool on your network. Routine security checks will provide resilience to your organization and prevent you from falling victim to a ransomware attack.

Below is additional guidance from the **HICP Publication Technical Volume #1: Cybersecurity Practices for Small Healthcare Organizations** on security protocols to help protect your small organization from ransomware attacks.

- **Establish and implement cybersecurity policies, procedures, and processes.** This is one of the most effective means of preventing cyberattacks. They set expectations and foster a consistent adoption of behaviors by your workforce.[3] Tech Volume 1-10.S.A
- **Become familiar with which data, applications, systems, and devices your contractors and vendors are authorized to access.**[3] If an attack takes place on you network, knowing who has access to your assets will enable you to triage the location in a more effective manner. Tech Volume 1-10.S.A
- **Schedule and conduct routine vulnerability scans on your network to detect technology flaws that hackers could exploit.** This process uses a scanning capability, often provided by a EHR or IT support vendor, to proactively scan devices and systems in your organization.[3] Tech Volume 1-7.S.A
- **Establish and implement an incident response plan.** Before an incident occurs, make sure you understand who will lead your incident investigation. Additionally, make sure you understand which personnel will support the leader during each phase of the investigation.[3] Tech Volume 1-8.S.A
- **Build a risk management process into your organization's structure.** A mature risk management program enables an organization to understand risks presented by Information and Communications Technology (ICT) products and services, including software, in the context of the mission or business processes they support."[2]
- **Create a strategy to review new vendors' security protocols** and implement compensating controls for deficiencies prior to enabling them access to your network and when purchasing third and fourth party services. Enabling a vetting process will help prevent data compromise and monitor risks that can happen due to fourth party relationships.

Additional Resources:

CISA and FBI have provided security guidelines that you can utilize to assist your organization if you have been affected by a supply chain attack.

CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack

Sources:

1. Scale, details of massive Kaseya ransomware attack emerge
2. Defending Against Software Supply Chain Attacks, April 2021, page 7
3. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients