THREAT BULLETINS

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

TLP:WHITE

Jul 06, 2021

On July 6, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) published the Current Activity regarding customers affected by the Kaseya VSA Supply-Chain Ransomware Attack. CISA and the FBI continue to respond to the recent supply-chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs) and their customers.

CISA and FBI strongly urge affected MSPs and their customers to follow the guidance below.

CISA and FBI recommend affected MSPs:

- Download the Kaseya VSA Detection Tool. This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.
- 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 allowlisting 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.

CISA and FBI recommend MSP customers affected by this attack take immediate action to implement the following cybersecurity best practices. **Note:** these actions are especially important for MSP customer who do not currently have their RMM service running due to the Kaseya attack.

CISA and FBI recommend affected MSP customers:

- Ensure backups are up to date and stored in an easily retrievable location that is air-gapped from the organizational network;
- Revert to a manual patch management process that follows vendor remediation guidance, including the installation of new patches as soon as they become available;
- Implement:
  - Multi-factor authentication; and
  - Principle of least privilege on key network resources admin accounts.

Health-ISAC's Threat Operations Center will continue to monitor the evolving incident and provide updates as they become available.

Reference(s)	box, cisa, kaseya

Sources
CISA-FBI Guidance for MSPs and Affected Customers

Kaseya VSA Detection Tool

Kaseya - Important Notice July 2nd, 2021

Alert ID 027b46c4

View Alert

Tags KASEYA

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**