An official website of the United States government Here's how you know

TLP:WHITE

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

Original release date: July 04, 2021

CISA and the Federal Bureau of Investigation (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.

Resources:

TLP:WHITE

TLP:WHITE

CISA and FBI provide these resources for the reader's awareness. CISA and FBI do not endo governmental entities nor guarantee the accuracy of the linked resources.

- For the latest guidance from Kaseya, see Kaseya's Important Notice July 3rd, 2021.
- For indicators of compromise, see Peter Lowe's GitHub page REvil Kaseya CnC Domains. **Note:** due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For guidance specific to this incident from the cybersecurity community, see Cado Security's GitHub page, Resources for DFIR Professionals Responding to the REvil Ransomware Kaseya Supply Chain Attack. **Note:** due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For advice from the cybersecurity community on securing against MSP ransomware attacks, see Gavin Stone's article, How secure is your RMM, and what can you do to better secure it?.
- For general incident response guidance, CISA encourages users and administrators to see Joint Cybersecurity Advisory AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE