BLOG

FAQ: Kaseya VSA Supply-Chain Ransomware Attack

By Risk Strategies Cyber Liability Practice

Jul 6, 2021

The United States Federal Bureau of Investigations, the Cybersecurity and Infrastructure Security Agency (CISA) and multiple media outlets have reported a supply-chain ransomware attack exploiting a vulnerability in Kaseya VSA software.

What Happened

On Friday, July 2nd, Kaseya, notified customers and posted a notice on their website regarding a possible attack against their VSA Software product. VSA is a unified remote-monitoring and management tool for handling networks and endpoints. It is primarily used by MSSP (Managed Security Service Provider) and enterprise clients.

Who is at Risk

Organizations that have either a Kaseya VSA server on-premise or that are managed remotely by a Managed Services Provider (MSP) that uses a VSA server.

Who's behind the attack

An affiliate of the notorious REvil gang, best known for extorting $11 million from the meat-processor JBS after a Memorial Day attack, infected thousands of victims in at least 17 countries on Friday, largely through firms that remotely manage IT infrastructure for multiple customers, cybersecurity researchers said. REvil's reported offer of a blanket decryption for all victims of the Kaseya attack in exchange for $70 million suggests an inability to cope with the sheer quantity of infected networks, said Allan Liska, an analyst with the cybersecurity firm Recorded Future. Although analysts reported seeing demands of $5 million and $500,000 for bigger targets, it was apparently demanding $45,000 for most.

How to protect/defend against this attack:

1. If using a Kaseya VGA On Premise product, disconnect it immediately. Per guidance by Kaseya, all on premises VSA Servers should continue to remain offline until further instructions from Kaseya about when it is safe to restore operations. A patch will be required to be installed prior to

restarting the VSA and a set of recommendations on how to increase your security posture will be provided by the company at a later date
2. Download and deploy Kaseya VSA Detention Tool to determine if any indicators of compromise are present
3. Enable and enforce multifactor authentication on every single account if possible
4. Implement “allowlisting” to limit communication with remote monitoring and management (RMM) capabilities to only known IP address pairs
5. Place administrative interfaces of RMM behind a VPN or firewall on a dedicated administrative network
6. Revert to manual patch management process that follow vendor remediation guidance
7. Ensure backups are up to date, stored in easily retrievable location, encrypted and air-gapped from the organizational network

What if you suspect unauthorized access?

Contact Risk Strategies and our breach response experts by email or by calling (844) 979-0265

References & Additional information

Kaseya ransomware supply chain attack: What you need to know, ZDnet, 7/85/21

Weekend sees single biggest global ransomware attack on record, Associated Press, 7/5/21

Kaseya Blog

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

Threat Brief: Kaseya VSA Ransomware Attacks

TAGS:
Cyber