



THREAT BULLETINS

CISA Current Activity - Kaseya VSA Supply-Chain Ransomware Attack



TLP:WHITE

Jul 02, 2021

On July 2, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) has published the Current Activity regarding the [Kaseya VSA Supply-Chain Ransomware Attack](#). CISA is taking action to understand and address the recent supply-chain ransomware attack against Kaseya VSA and the multiple MSPs that employ VSA software. CISA encourages organizations review the [Kaseya advisory](#) and immediately follow their guidance to shutdown VSA servers.

Kaseya released an important notice stating they are experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers as of 2:00 PM EDT today July 2, 2021. The statement is as follows:

"We are in the process of investigating the root cause of the incident with an abundance of caution, **but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us.**

Its critical that you do this immediately, because one of the first things the attacker does is shutoff administrative access to the VSA."

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

[Kaseya VSA Supply-Chain Ransomware Attack](#)

[Kaseya - Important Notice July 2nd, 2021](#)

[REvil ransomware attacks systems using Kaseya's remote IT management software](#)

[Reddit - Critical Ransomware Incident in Progress](#)

[MSSP Alert](#)

[Kaseya hit with suspected cyberattack, raising fears of major supply chain incident](#)

Reference(s)

[cisa](#), [Reddit](#), [kaseya](#), [Cyberscoop](#), [MSSP Alert](#), [The Verge](#)

Sources

[Kaseya VSA Supply-Chain Ransomware Attack](#)

[Kaseya - Important Notice July 2nd, 2021](#)

[REvil ransomware attacks systems using Kaseya's remote IT management software](#)

[Reddit - Critical Ransomware Incident in Progress](#)

[MSSP Alert](#)

[Kaseya hit with suspected cyberattack, raising fears of major supply chain incident](#)

Alert ID 0739ee72

[View Alert](#)

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>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.