ProTelesis
Global IT Innovation

Dear Valued Customer,

As a full service IT providers, ProTelesis goes through great lengths to keep your business secure. To that end, ProTelesis is taking action to understand and address the recent supply-chain ransomware attack against Kaseya VSA (Virtual System Administrator) and the multiple managed service providers (MSPs) that employ VSA software. As a result, ProTelesis shutdown it's Kaseya servers on 2:43PM Mountain Time on Friday 7/2/2021 and currently has no plan to turn them back on. At this time, we have zero reports of any of our customers being compromised or ransomware deployed through our Kaseya VSA servers when they were online.

Even though the Kaseya Agent is not believed to have been compromised, we implemented and deployed an uninstaller script to remove the Kaseya Agent from customer systems. This was performed over weekend and is running daily via our Datto RMM agent that we started deploying months ago as part of our efforts to decommission the Kaseya VSA software. We suggest that customers confirm that the Kaseya Agent has been uninstalled or manually uninstall the Kaseya agent if needed.

What Happened?

Kaseya is urging MSPs to immediately shut down on-premises VSA servers amid a potential cyberattack that may be targeting the RMM (remote monitoring and management) software.

The CISA (Cybersecurity and Infrastructure Security Agency) has issued an alert about the attack, stating that the agency is monitoring details about a "supply-chain ransomware attack against Kaseya VSA and multiple managed service providers (MSPs) that employ VSA software."

Kaseya has stated they are in the process of investigating the root cause of the incident with an abundance of caution, but they are recommending all customers IMMEDIATELY shutdown their VSA server until further notice.

Key Points To Know

- According to a report from Bleeping Computer, the attack targeted six large MSPs and has encrypted data for as many as 1000 companies.
- The attack has been linked to the notorious REvil ransomware gang (already linked to attacks on Acer and meat supplier JBS earlier this year)
- Delivery appears to be via an automated software update or exploit in Kaseya (which had an earlier, smaller, ransomware incident in 2019). The attacker immediately stops administrator access to the VSA.
- These files are dropped on the client systems:
- agent.exe (dropper): d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
- mpsv.dll: 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
- By design Kaseya allows administration of systems with high level privilege's so the potential for ransomware to propagate is high.

ProTelesis
Global IT Innovation

Additional Resources

- Kaseya Security Notice: https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689

Kaseya Compromise Detection Tool Request

Syed Rahil (Kaseya)

Jul 6, 2021, 1:03 PM EDT

Here is the link where you can download the instructions and scripts to be run on your Kaseya server (where the VSA is hosted, if applicable) and on any agent you would like to check. **NOTE**: Make sure the VSA remains isolated and off the internet.

https://kaseya.box.com/s/p9b712dcwfsnhuq2jmx31ibsuef6xict

- Please watch the Install Guide video ***before*** running the scripts.
- Download the instructions in the zip file.
- Download the file locally and move the *VSA Detection Tools.zip* into the Kaseya Server.
- Download the file locally and move the *Endpoint Detection folder* to any agent.

Please note that regardless of the results of the detection tool, please keep the VSA offline and isolated until further notice.

If you encounter any errors while running the scripts, please refer to point 5a in the instructions PDF.

Thank you,

Syed Rahil | Syed Rahil K| Customer
Support Engineer

Email: syed.k@kaseya.com