July 13, 2021

Kaseya - Releases Security Updates for Critical Security Vulnerabilities in VSA Servers, Restores Services for On-Premise and SaaS Customers

Content

Kaseya's Updates on Ransomware Attack:

- On July 12, 2021, Kaseya released security updates for critical security vulnerabilities in Virtual System Administrator (VSA) responsible for the ransomware attack on July 02, 2021
- The attack was launched by a ransomware group called REvil by using the VSA vulnerabilities against the company's Material Service Providers (MSPs) and their customers
- Approximately 60 MSP's and 1,500 businesses across the globe have been impacted
- REvil demanded a ransom of US$70 M for a universal decryption key
- Immediately after the attack, Kaseya had urged its software-as-a-service version (SaaS) customers to shut down their VSA servers until a patch was available
- On July 6, 2021, initial attempts to relaunch SaaS servers were made by the company, which was delayed due to technical issues
- On July 11, 2021, the company released the patch to VSA on-premise customers and restoration of services were in progress, with 60% of the company's SaaS customers going live
- On July 12, 2021, the company reported that the restoration of VSA SaaS services were complete, with 100% of its SaaS customers going live
- Kaseya also reported that the unplanned maintenance across the VSA SaaS infrastructure has completed and all instances are live
- However, it may take some time for on-premise customers such as MSP's to apply the update and restore services to their customers
- Additionally, support teams were also assisting organizations in applying the security update

Fixed Security Vulnerabilities:

- The security updates in latest version, VSA version 9.5.7a (9.5.7.2994) includes fixes for three new security flaws as listed below:
    - CVE-2021-30116: Credential's leak and business logic flaw
    - CVE-2021-30119: Cross-site scripting vulnerability
    - CVE-2021-30120: Two-factor authentication bypass
- The updates also resolve three other vulnerabilities including:
    - A secure flag problem in User Portal session cookies
    - A bug that exposed weak password hashes in certain application programming interface (API) responses to brute-force attacks
    - A vulnerability that could allow the unauthorized upload of files to the VSA server
- The vulnerabilities that were fixed in previous VSA Releases in April 2021 include:
    - CVE-2021-30117: SQL injection vulnerability
    - CVE-2021-30118: Remote code execution vulnerability
    - CVE-2021-30121: Local file inclusion vulnerability
    - CVE-2021-30201: XML external entity vulnerability

Implementation of Additional Security Measures:

- Kaseya is limiting access to the VSA web graphical user interface (GUI) to local IP addresses
- Due to the speed necessary in deploying the patch, some VSA functionality has been disabled temporarily, including some API endpoints

- Kaseya said the API calls are being redesigned for the highest level of security
- The company has also temporarily removed the ability to download agent installer packages without authentication to VSA and the User Portal page
- A number of legacy functions have been permanently removed
- Customers need to change their password once they have installed and logged in to the latest build
- Kaseya has also provided VSA SaaS and on-premise hardening and best practice guides

Steps to Resume VSA Servers and Connecting to the Internet:

- Ensure VSA server is isolated
- Check System for Indicators of Compromise (IOC)
- Patch the Operating Systems of the VSA Servers
- Using URL Rewrite to control access to VSA through IIS server
- Install FireEye Agent
- Remove Pending Scripts/Jobs

New Features:

- In this release, the company added new functionality for a VSA admin to control certain end-user inputs so that the VSA admin can work on the remote device without disruption by an end-user
- A feature to lockout keyboard and mouse from being able to be used by end-user
- Removed menu items from the Remote-Control toolbar if the feature is not supported for a given VSA Agent type

Accusations Against Kaseya:

- Former employees of Kaseya have claimed that the company knew about the critical flaws in their software between 2017 and 2020, but ignored them
- The employees also reported that the use of outdated code, weak encryption and passwords in Kaseya's products and servers accounted for the ransomware attack
- The company failed to adhere to basic cybersecurity practices such as regularly patching software
- If these accusations are proved, Kaseya is expected to face issues with regulations such as European Union General Data Protection Regulation and the California Consumer Privacy Act
- Supply Wisdom is continuously monitoring the situation and will alert you to any relevant developments

Maintaining Business Continuity and Resilience Amid Increased Cyberattacks

- Supply Wisdom is recommending the following best practices to our clients to minimize business disruption risks:
  - It is important for clients to determine whether all of Kaseya’s recommended mitigation steps and mandated upgrades are assessed and implemented
  - On-Premise customers are advised to follow the instructions in the “On-Premises VSA Startup Readiness Guide” (https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993), and review the “VSA On-Premises Hardening and Best Practice Guide” (https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417) , prior to deploying the VSA 9.5.7a release
  - SaaS customers are advised to follow the instructions in the “VSA SaaS Startup Guide” (https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369), and review the “VSA SaaS Security Best Practices Guide” (https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009) after SaaS instance is available
  - Clients are advised to view the Kaseya VSA Security page (https://www.kaseya.com/potential-attack-on-kaseya-vsa/) to follow the updates regarding the VSA security incident
  - It is recommended for clients to regularly audit applications which are installed in the devices and review all internal, sourcing, and service partners' networks, and ensure that they have completed the required patches and updates
  - Determine if the third party regularly tests its networks for vulnerabilities and potential risks and errors and has a well-documented response plan in place, which helps it detect glitches as well as notify concerned parties in a timely and effective manner
  - Clients should request the third party to share results of vulnerability tests with them without fail
  - Clients should also review the Business Continuity Plan or Disaster Recovery policies of the third parties and enquire if cybersecurity-related incidents are included in the same to keep operations secured and uninterrupted
  - It is advised to follow similar alerts monitored by Supply Wisdom, regularly check advisories issued or emailed directly by Kaseya, and follow any other instructions provided by the third party

    - In the era of widespread prevalence of cyber-security threats, it is crucial for clients to have an independent cyber assessment of the concerned third parties done on a real-time basis, such as the cyber susceptibility review service from Supply Wisdom, which has been designed to ensure that clients have necessary information about the cyber health of their third-parties

Source(s)

- https://thehackernews.com/2021/07/kaseya-releases-patches-for-flaws.html
- https://www.zdnet.com/article/kaseya-issues-patch-for-on-premise-customers-saas-rollout-underway/
- https://www.bleepingcomputer.com/news/security/kaseya-patches-vsa-vulnerabilities-used-in-revil-ransomware-attack/
- https://venturebeat.com/2021/07/12/with-kaseya-patch-it-teams-begin-the-long-slog-to-recovery/
- https://www.kaseya.com/potential-attack-on-kaseya-vsa/
- https://siliconangle.com/2021/07/12/kaseya-release-patch-restores-services-following-revil-ransomware-attack/
- https://helpdesk.kaseya.com/hc/en-gb/articles/229026328-Patch-Release-Process-VSA-Patch-Installation-instructions
- https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-12th-2021
- https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041-9-5-7a-9-5-7-2994-Feature-Release-11-July-2021-
- https://us-cert.cisa.gov/ncas/current-activity/2021/07/12/kaseya-provides-security-updates-vsa-premises-software