Update Regarding VSA Security Incident

kaseya.com/potential-attack-on-kaseya-vsa/

Updates Regarding VSA Security Incident

July 26, 2021 - 1:00 PM EDT

Throughout this past weekend, Kaseya's Incident Response team and Emsisoft partners continued their work assisting our customers and others with restoration of their encrypted data. We continue to provide the decryptor to customers that request it, and we encourage all our customers whose data may have been encrypted during the attack to reach out to your contacts at Kaseya. The decryption tool has proven 100% effective at decrypting files that were fully encrypted in the attack.

Kaseya has maintained our focus on assisting our customers, and when Kaseya obtained the decryptor last week we moved as quickly as possible to safely use the decryptor to help our customers recover their encrypted data. Recent reports have suggested that our continued silence on whether Kaseya paid the ransom may encourage additional ransomware attacks, but nothing could be further from our goal. While each company must make its own decision on whether to pay the ransom, Kaseya decided after consultation with experts to not negotiate with the criminals who perpetrated this attack and we have not wavered from that commitment. As such, we are confirming in no uncertain terms that Kaseya did not pay a ransom – either directly or indirectly through a third party – to obtain the decryptor.

July 23, 2021 - 3:00 PM EDT

Kaseya's Incident Response team, assisted by Emsisoft, continues to provide our customers with the decryption key and help them to restore any encrypted data that was not previously restored from backup. We have no reports of problems or issues with the decryptor.

July 22, 2021 - 3:30 PM EDT

Kaseya has obtained universal decryptor key.

On 7/21/2021, Kaseya obtained a decryptor for victims of the REvil ransomware attack, and we're working to remediate customers impacted by the incident.

We can confirm that Kaseya obtained the tool from a third party and have teams actively helping customers affected by the ransomware to restore their environments, with no reports of any problem or issues associated with the decryptor. Kaseya is working with Emsisoft to support our customer engagement efforts, and Emsisoft has confirmed the key is effective at unlocking victims.

We remain committed to ensuring the highest levels of safety for our customers and will continue to update here as more details become available.

Customers who have been impacted by the ransomware will be contacted by Kaseya representatives.

July 19, 2021 - 3:15 PM EDT

VSA 9.5.7.3011 Maintenance Patch Release Update

Kaseya is releasing patch 9.5.7.3011 which remediates functionality issues caused by the enhanced security measures put in place and provides bug fixes (this is not a security release). The full release notes with the fixes are available at: https://helpdesk.kaseya.com/hc/en-gb/articles/4404146456209.

VSA SaaS Update

The first VSA SaaS deployment went live on Saturday July 17th US EDT for the following VSA SaaS instances: EU – SAAS03, EU – SAAS06, EU – SAAS11, EU – SAAS12, EU – SAAS16, EU – SAAS23, EU – SAAS24, EU – SAAS25, EU – SAAS28, EU – SAAS34, EU – SAAS39, EU – SAAS41 ,EU – SAAS43, US – NA1VSA01, US – NA1VSA04, US – NA1VSA08, US – NA1VSA12, US – NA1VSA14, US – NA1VSA22, US – NA1VSA28, US – NA1VSA29, US – NA1VSA30, US – NA1VSA32, US – NA1VSA37, NA1VSA105, US – NA1VSA108, US – NA1VSA115, US – IAD2VSA02, US – IAD2VSA04

The remainder of the VSA SaaS instances will be updated tonight (July 19th) 8PM and 4AM US EDT.

VSA On-Premises Update:

The VSA On-Premises Patch will be released to customers and posted to the download site by 4:30PM US EDT today.

July 16, 2021 - 7:00 PM EDT

VSA 9.5.7.3011 Maintenance Patch Release Update

Kaseya will be releasing patch 9.5.7.3011 which remediates functionality issues caused by the enhanced security measures put in place and provides bug fixes (this is not a security release). (this is **not** a security release). The full release notes with the fixes are available at: https://helpdesk.kaseya.com/hc/en-gb/articles/4404146456209.

The patch is planned to be available for VSA On-Premises customers by Monday July 19th end of day.

The first VSA SaaS deployment is planned for Saturday July 17th between 7AM and 11AM US EDT for the following VSA SaaS instances: EU – SAAS03, EU – SAAS06, EU – SAAS11, EU – SAAS12, EU – SAAS16, EU – SAAS23, EU – SAAS24, EU – SAAS25, EU – SAAS28, EU – SAAS34, EU – SAAS39, EU – SAAS41 ,EU – SAAS43, US – NA1VSA01, US – NA1VSA04, US – NA1VSA08, US – NA1VSA12, US – NA1VSA14, US – NA1VSA22, US – NA1VSA28, US – NA1VSA29, US – NA1VSA30, US – NA1VSA32, US – NA1VSA37, NA1VSA105, US – NA1VSA108, US – NA1VSA115, US – IAD2VSA02, US – IAD2VSA04

The remainder of the VSA SaaS instances are planned for deployment between 8PM and 4AM US EDT on Monday July 19th.

July 14, 2021 - 5:00 PM EDT

VSA Install Patch Check

When running the Kinstall patch on your VSA, if you chose to reinstall VSA and either **unchecked** the default option to install the latest patch, or **reran** the Reinstall VSA process a 2nd time **without** the “install patch” option selected – it’s possible your patch was not re-applied.

While these are rare edge cases, we recommend that you verify that the latest patch was installed properly. We have made a tool that enables you to ensure the patch is properly install.

Download the verification tool at:
https://app.box.com/s/5kqsbdj9aajezsc63jzaadpka5esk1v8

July 13, 2021 - 8:00 PM EDT

VSA Update:

Version 9.5.7a was released to both VSA SaaS and On-Premises on Sunday July 11th.

Please ensure you have reviewed the release notes at: https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041

Additionally, we recommend reviewing the following documents:

VSA On-Premises Integration IP Whitelist – https://helpdesk.kaseya.com/hc/en-gb/articles/4403869952657

On Premises Startup Runbook (Updated July 11th – Updated Step 4) – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993incident-response

VSA On-Premise Hardening and Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

VSA SaaS Startup Runbook – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

VSA SaaS Hardening and Best Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

July 12, 2021 - 3:30 PM EDT

The unplanned maintenance across the VSA SaaS infrastructure has completed and all instances are now live.

With the large number of users coming back online in a short window, we had seen some performance issues. We made configuration changes to address the issue and it is now resolved. We will continue to monitor the performance and make adjustments as required.

July 12, 2021 - 12:15 PM EDT

Unplanned maintenance will be performed across the entire SaaS farm today, between 12:00 PM to 2:00 PM EDT with an expected downtime of 20 minutes. With the large number of users coming back online in a short window, we have seen some performance issues. We made some configuration changes to address and need to restart the servers for these to take effect and improve performance.

July 12, 2021 - 8:00 AM EDT

VSA Update:

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS Infrastructure prior to the 4:00 PM target. The restoration of services is now complete, with 100% of our SaaS customers live as of 3:30 AM US EDT. Our support teams continue to work with VSA On-Premises customers who have requested assistance with the patch.

We will continue to post updates as new information becomes available.

July 12, 2021 - 3:00 AM EDT

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS Infrastructure prior to the 4:00 PM target. The restoration of services is progressing, with 95% of our SaaS customers live and servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.

We will continue to post updates on the patch rollout progress and server status.

July 11, 2021 - 10:00 PM EDT

VSA Update:

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS Infrastructure prior to the 4:00 PM target. The restoration of services is progressing according to plan, with 60% of our SaaS customers live and servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.

We will continue to post updates on the patch rollout progress and server status throughout the evening.

July 11, 2021 - 4:30 PM EDT

VSA Update:

VSA SaaS and On-Premises Release Notes have now been published and are available at: https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041

VSA SaaS:

The restoration of our VSA SaaS Infrastructure has begun. We will send email notifications as the individual instances come back online over the next several hours.

Please review:

VSA SaaS Startup Runbook – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

VSA SaaS Hardening and Best Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

VSA On-Premises

The VSA On-Premises patch is now available. You can run KINSTALL as you normally do as part of your patching process.

Please review:

On Premises Startup Runbook (Updated July 11th – Updated Step 4) – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993incident-response

VSA On-Premise Hardening and Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

Kaseya EVP Mike Sanders Provides Situational Update for VSA Readiness - July 11, 2021 12:15 PM EDT

Kaseya's technical teams are finalizing both the on-premises patch and SaaS platform updates in preparation for 4:00 PM EDT release. Mike Sanders provides an update and notes recent updates to the On-Premises Runbook (https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993incident-response,) also noted on this page below.

July 11, 2021 - 10:30 AM EDT

VSA Update:

We remain on track to release the VSA On-Premises Patch and begin bringing our VSA SaaS Infrastructure online on Sunday, July 11th at 4 PM EDT.

NEW – We have updated our VSA On-Premises runbook **STEP 4** – Based on customer feedback, we have made changes to the IIS rewrite tool in order to give customers more control of their environments using their firewalls. Please review **STEP 4** in the document at the following link: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

NEW – We have updated our VSA On-Premises runbook to include a tool that you can use to clear any procedures that have accumulated prior to starting restarting your VSA. Please review **STEP 6** in the document at the following link: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

Continued Updates

Please ensure you have reviewed the following documents:

VSA On-Premises:

On Premises Startup Runbook (Updated July 11th – Updated Step 4) – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993incident-response

VSA On-Premise Hardening and Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

VSA SaaS:

VSA SaaS Startup Runbook – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

VSA SaaS Hardening and Best Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

Kaseya EVP Mike Sanders Provides Situational Update for VSA Readiness - July 10, 2021 3:30 PM EDT

Kaseya's technical teams and their partners are actively testing the updates and will continue to do so over the next 24 hours. Mike Sanders updates on progress and provides guidance for customers in advance of tomorrow's release.

July 10, 2021 - 2:00 PM EDT

VSA Update:

We remain on track to release the VSA On-Premises Patch and begin deployment to our VSA SaaS Infrastructure on Sunday, July 11th at 4 PM EDT.

Later this evening, we will provide the latest status update video from our Executive Vice President, Mike Sanders, on our incident response and the steps you can take now to be ready for the release.

For our VSA On-Premises customers, we will be releasing a tool shortly that will clear any pending procedures and that will be included in the runbooks below – stay tuned.

Continued Updates

Please ensure you have reviewed the following documents:

VSA On-Premises:

On Premises Startup Runbook (Updated July 9th – Added Step 7) – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993incident-response

VSA On-Premise Hardening and Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

VSA SaaS:

VSA SaaS Startup Runbook – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

VSA SaaS Hardening and Best Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

July 10, 2021 - 9:30 AM EDT

VSA Update:

We remain on track to release the VSA On-Premises Patch and begin deployment to our VSA SaaS Infrastructure on Sunday, July 11th at 4 PM EDT.

Please ensure you have reviewed the following documents:

VSA On-Premises:

On Premises Startup Runbook (Updated July 9th – Added Step 7) – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

VSA On-Premise Hardening and Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

VSA SaaS:

VSA SaaS Startup Runbook – https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

VSA SaaS Hardening and Best Practice Guide – https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

July 9, 2021 - 7:00 PM EDT

Reminder: Spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments or phone claiming to be Kaseya Partners – **DO NOT** click on links or download attachments and **DO NOT** respond to phone calls claiming to be a Kaseya Partner.

Updates:

Sunday, July 11th at 4 PM EDT the VSA On-Premises Patch will be available and we will start the deployment to our VSA SaaS Infrastructure.

We have updated our VSA On-Premise Hardening and Practice Guide (added Step #7) which can be viewed by visiting: released and can be reviewed by visiting: https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

Kaseya EVP Mike Sanders Provides Situational Update for VSA Readiness - July 9, 2021 6:00 PM EDT

Kaseya’s technical teams and their partners continue to work toward getting customers back up and running. EVP Mike Sanders explains progress to date, and raises awareness of suspicious communications coming from outside Kaseya.

July 9, 2021 - 5:00 PM EDT

As previously communicated, spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments.

Spammers may also be making phone calls claiming to be a Kaseya Partner reaching out to help.

Kaseya **IS NOT** having any partners reach out – **DO NOT** respond to any phone calls claiming to be a Kaseya Partner.

DO NOT click on any links or download any attachments in emails claiming to be a Kaseya advisory. However, some customers have subscribed to our support site and, at this point, those automated emails may contain links. As precaution, be careful with any links or attachments in any emails.

New Updates:

We will be providing a video update from our Executive Vice President, Mike Sanders, later this evening with an update on the incident, our response, and our release planned for this Sunday at 4PM US EDT.

We have updated our VSA On-Premises Hardening and Practice Guide (added Step #7) which can be viewed by visiting: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

July 9, 2021 - 12:00 PM EDT

As previously communicated, spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments.

Spammers may also be making phone calls claiming to be a Kaseya Partner reaching out to help.

Kaseya **IS NOT** having any partners reach out – **DO NOT** respond to any phone calls claiming to be a Kaseya Partner.

DO NOT click on any links or download any attachments in emails claiming to be a Kaseya advisory.

July 9, 2021 - 9:00 AM EDT

As previously communicated, spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments.

Do not click on any links or download any attachments in emails claiming to be a Kaseya advisory.

Moving forward, all new Kaseya email updates **will not contain any links or attachments**.

VSA Incident Update:

***New** – VSA On-Premise Hardening and Practice Guide was released and can be reviewed at: https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

Reminders:

If you have not reviewed the runbooks for the upcoming release, links to them are below:

VSA On-Premise Runbook: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

VSA SaaS Runbook: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

Kaseya CTO Dan Timpson Addresses Progress to Date and Next Steps for VSA - July 8, 2021 5:00 PM EDT

Kaseya's technical teams and their partners have been working around the clock to help affected customers get back up and running. CTO Dan Timpson talks about the agency, incident response and research partners who are assisting Kaseya's internal teams to ensure the highest levels of security prior to go-live and outlines the steps Kaseya is taking to ensure its VSA customers get back online securely. He further discusses the contained impact to VSA within the IT Complete platform and the intentional compartmentalized design that ensures the security of the remaining 26 modules within the platform.

July 8, 2021 - 1:30 PM EDT

Earlier today we released a video post form our CEO updating the patch rollout timeline as follows:

Sunday July 11th at 4PM EDT the On-Premises Patch will be available and we will start the deployment to our VSA SaaS Infrastructure.

We will be providing a video update from our CTO later this evening which will be emailed to VSA customers providing further technical clarity. We will continue to provide both text and daily video updates from executives as we move forward toward release this Sunday.

We have also updated our runbooks for customers to prepare for the rollout and restoration of service. If you have not reviewed the runbook, please ensure you review the links below (please note we will send notifications in future email updates if runbooks are updated with additional information):

For our **VSA On-Premises** customers, we have now have published a runbook of the changes to make to your on-premises environment so customers can prepare for the patch release. Here is the link to the runbook (https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993).

For our **VSA SaaS** customers, we have published a runbook to help you prepare for the steps you can take after the SaaS environment returns to service at: https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

July 7, 2021 - 9:45 PM EDT

For our VSA On-Premises customers, we have now have published a runbook of the changes to make to your on-premises environment so customers can prepare for the patch release. Here is the link to the runbook **(https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993).**

We are in the process of resetting the timelines for VSA SaaS and VSA On-Premises deployment. We apologize for the delay and changes to the plans as we work through this fluid situation.

We will be providing a video update from our CEO later this evening which will be emailed to VSA customers providing further clarity.

Important Message from Kaseya CEO Fred Voccola - July 7, 2021 8:00 PM EDT

July 7, 2021 - 7:00 PM EDT

We are in the process of resetting the timelines for VSA SaaS and VSA On-Premises deployment. We apologize for the delay and changes to the plans as we work through this fluid situation.

We will be providing a video update from our CEO later this evening which will be emailed to VSA customers providing further clarity.

For our VSA On-Premises customers, we will be publishing a runbook of the changes to make to your on-premises environment on this site later this evening customers can prepare for the patch release.

July 7, 2021 - 3:00 PM EDT

The detailed runbook to prepare an On Premise VSA implementation for the new release is being finalized. This runbook is being emailed to you, and it will be posted on our support website.

The runbook consists of the following:

- Steps to Isolate the VSA server from the network and the internet
    How to Run the Detection Tool
        The link to the detection tool is below as part of previous updates
- Steps to patch your operating system to ensure it is up to date
- Detailed review of the required changes to IIS
- How to download of the FireEye agent on the VSA Server
- How to implement the FireEye agent on the VSA Server
- Final review of the checklist before the installation of the new VSA release

The next update for On Premise VSA Customers is scheduled for 6pm tonight. This update will include the timing of the new VSA release for On Premise VSA Customers.

July 7, 2021 - 12:00 PM EDT

VSA On-Premises Update

- For on-premises customers we will be publishing a runbook of the changes to make to your on-premises environment by 3PM US EDT today so customers can prepare for the patch release.
- We will update the planned availability of the VSA On-Premises patch by 5PM US EDT today.

VSA SaaS Update

> During the VSA SaaS deployment an issue was discovered that has blocked the release. We are resolving the issue that is related to our SaaS infrastructure and we plan on beginning to restore SaaS services no later than the evening of Thursday July 8th US time.

July 7, 2021 - 8:00 AM EDT

As communicated in our last update, unfortunately, during the deployment of the VSA update an issue was discovered that has blocked the release. We have not yet been able to resolve the issue. The R&D and operations teams worked through the night and will continue to work until we have unblocked the release. We will provide a status update at 12:00PM US EDT.

July 6, 2021 - 10:00 PM EDT

During the VSA SaaS deployment an issue was discovered that has blocked the release. Unfortunately, the VSA SaaS rollout will not be completed in the previously communicated timeline. We apologize for the delay and R&D and operations are continuing to work around the clock to resolve this issue and restore service. We will be providing a status update at 8AM US EDT.

July 6, 2021 - 7:30 PM EDT

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 6, 2021 5:00 PM EDT and earlier updates.

- The technical work for SaaS Deployment has started at 4:00 PM EDT and will continue for the next several hours pending no issues.

- We are configurating an additional layer of security to our SaaS infrastructure which will change the underlying IP address of our VSA servers (the domain names/URL will not change) For almost all customers, this change will be transparent. However if, and only if, you have whitelisted your Kaseya VSA server in your firewall(s), you will need ot update the IP whitelist. The new IP addresses can be found at: https://www.cloudflare.com/ips/
- No SaaS VSA services are on-line as of 7:30 PM. The enhanced security measures are currently being implemented and verified for proper operation. Once operational, we will then publish the VSA availability timeline. We will be updating the support web page hourly at *https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689*
- Our On-Premises patch timeline is 24 hours (or less) from the restoration of SaaS services. We are focused on shrinking this time frame to the minimal possible – but if there are any issues found during the spin-up of SaaS, we want to fix them before bringing our on-premises customers up.

Continued Advisory

- 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.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**

July 6, 2021 - 5:00 PM EDT

Good progress being made. The next update will be posted by 6:00 PM.

July 6, 2021 - 12:00 PM EDT

Next Update is planned to be published July 6th between 2:00 PM and 5:00 PM EDT.

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 5, 2021 9:30 PM EDT and earlier updates.

- **Our Timeline for bringing SaaS servers on-line has shifted out by two hours – it is now July 6th between 4:00 PM EDT and 7:00 PM EDT due to configuration change and enhanced security measures being put in place.**

- **Our On-Premises patch timeline is 24 hours (or less) from the restoration of SaaS services. We are focused on shrinking this time frame to the minimal possible – but if there are any issues found during the spin-up of SaaS, we want to fix them before bringing our on-premises customers up.**
- **The enhanced security measures that will be brought online are:**
  - 24/7 Independent SOC for every VSA with the ability to quarantine and isolate files and entire VSA servers.
  - A complementary CDN with WAF for every VSA (Including on premise that opt-in and wish to use it – details will be available in a KB later this afternoon).
  - Customers who whitelist IPs will be required to need to whitelist additional IPs.
  - A new KB article on the SOC, CDN, and Whitelisting details will be published later this afternoon and linked to this KB on the Kaseya website.
  - Greatly reduces the attack surface of Kaseya VSA overall.
- **Later today we will release a customer-ready statement for you to use to communicate to your customers on the incident and the security measures that we have put in place.**
- A Compromise Detection Tool can be downloaded at the following link: VSA Detection Tool | Powered by Box. This continues to be enhanced, so please refer to the download site for the latest version.
- Incident Update – more details can be found here: Incident Overview & Technical Details – Kaseya
- To date, we are aware of fewer than 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by this attack. While many of these customers provide IT services to multiple other companies, we understand the total impact thus far has been to fewer than 1,500 downstream businesses.
- We have not found evidence that any of our SaaS customers were compromised.
- VSA is the only Kaseya product affected by the attack and all other IT Complete modules are not impacted.

Continued Advisory

- 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.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**

July 5, 2021 - 9:30 PM EDT

Next Update is planned to be published July 6th between 8:00 AM and 12:00 PM EDT.

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 5, 2021 1:00 PM EDT and earlier updates.

- Incident Update
  - In an effort to be transparent with our customers, Kaseya is sharing the information concerning the recent ransomware attack in an Incident Overview & Technical Details document which is available at this link.
  - To date, we are aware of fewer than 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by this attack. While many of these customers provide IT services to multiple other companies, we understand the total impact thus far has been to fewer than 1,500 downstream businesses. We have not found evidence that any of our SaaS customers were compromised.
  - We have had no new reports filed of compromises for VSA customers since Saturday July 3rd.
  - VSA is the only Kaseya product affected by the attack and all other IT Complete modules are not impacted.
  - An article by Reuters covers the incident – link
- Our executive committee met this afternoon at 6:30 PM EDT to reset the timeline and process for bringing our SaaS and on-premises customers back online.
  - The Patch for on-premises customers has been developed and is currently going through the testing and validation process. We expect the patch to be available within 24 hours after our SaaS servers have been brought up.
  - The current estimate for bringing our SaaS servers back online is July 6th between 2:00 PM – 5:00 PM EDT. A final go/no-go decision will be made tomorrow morning between 8:00 AM EDT – 12:00 AM EDT. These times may change as we go through the final testing and validation processes.
- We will be releasing VSA with staged functionality to bring services back online sooner. The first release will prevent access to functionality used by a very small fraction of our user base, including:
  - Classic Ticketing
  - Classic Remote Control (not LiveConnect).
  - User Portal
- Kaseya met with the FBI/CISA tonight to discuss systems and network hardening requirements prior to service restoration for both SaaS and on-premises customers. A set of requirements will be posted prior to service restart to give our customers time to put these counter measures in place in anticipation of a return to service on July 6th.

- A new version of the Compromise Detection Tool can be downloaded at the following link: VSA Detection Tools.zip | Powered by Box
  - This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.
  - The latest version searches for the indicators of compromise, data encryption, and the REvil ransom note. We recommend that you re-run this procedure to better determine if the system was compromised by REvil.
  - Over 2,000 customers have downloaded this tool since Friday.

Continued Advisory

- 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.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**

July 5, 2021 - 1:00 PM EDT [Updated at 6:30 PM EDT]

Next Update is planned to be published July 5th between 5:00 PM and 7:00 PM 7:00 PM and 8:00 PM EDT.

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 4, 2021 11:00 PM EDT and earlier updates.

- We will be providing a separate update with more technical details of the incident to aid our customers and security researchers during the afternoon of July 5th.

- SaaS Restoration Timeline Updates – UPDATE
    - Our executive committee met this morning at 8:00 AM EDT, and to best minimize customer risk, felt that more time was needed before we brought the data centers back online.
    - They elected to meet again later this afternoon at 3:00 PM EDT to reset the schedule for starting the restoration process to bring our datacenters online. We will provide an updated timeline at approximately 5:00 PM – 7:00 PM EDT today (July 5th).
    - We are in the midst of deploying an enhanced security monitoring infrastructure and are testing the revised incident response processes and performance management controls to ensure acceptable operations for our customers.
    - The next update will be later this evening (EDT) after the executive committee reconvenes.
- On-Premises Patch Timeline Updates – NEW

    We are developing the new patch for on-premises clients in parallel with the SaaS Data Center restoration. We are deploying in SaaS first as we control every aspect of that environment. Once that has begun, we will publish the schedule for distributing the patch for on-premises customers.
- The Compromise Detection Tool can be download at the following link: VSA Detection Tools.zip | Powered by Box This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.

Continued Advisory

- 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.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**

July 5, 2021 - 11:00 AM EDT

A revision to this update is coming later today. Please check back at approximately 1:00 PM EDT.

July 4, 2021 - 11:00 PM EDT

Next Update is planned to be published July 5th in the morning EDT. The update will be published on the Kaseya.com support website (link here) in advance of the email being sent. Checking this link is the fastest way to ensure that you have the latest information from Kaseya.

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 4, 2021 5:45 PM EDT and earlier updates.

- SaaS Restoration Timeline Updates – UPDATE
  - Our executive committee met at 10:00 PM EDT and to best minimize customer risk, felt that more time was needed before we brought the data centers back online.
  - They elected to meet again tomorrow morning at 8:00 AM EDT to reset the schedule with a goal of starting the restoration process to bring our datacenters online by end of day on July 5th local time (UTC) – but that timeframe is dependent on achieving some key objectives overnight.
  - The next update will be tomorrow morning EDT after the executive committee reconvenes.
- On-Premises Patch Timeline Updates – NEW

  Once we have begun the SaaS Data Center restoration process (see SaaS Restoration Timeline Updates above), we will publish the schedule for distributing the patch for on-premises customers.

Continued Advisory

- 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.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**
- The new Compromise Detection Tool can be download at the following link: VSA Detection Tools.zip This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.

July 4, 2021 - 5:30 PM EDT

Next Update will be published July 4th in the very late evening EDT. Checking this link is the fastest way to ensure that you have the latest information from Kaseya.

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Our security, support R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service.

This update provides further detail on the July 4, 2021 10:00AM EDT and earlier updates.

Our efforts have shifted from root cause analysis and mitigating the vulnerability to beginning the execution of our service recovery plan. This plan will consist of the following stages:

Communication of our phased recovery plan with SaaS customers first followed by on-premises customers.

- In the spirit of responsible disclosure, Kaseya will be publishing a summary of the attack and what we have done to mitigate it.
- Some lightly-used legacy VSA functionality will be removed as part of this release out of an abundance of caution. A specific list of the functionality and its impact on VSA capabilities will be outlined in the release notes.
- There will be new security measures implemented including enhanced security monitoring of our SaaS servers by FireEye and enablement of enhanced WAF capabilities.
- We have successfully completed an external Vulnerability Scan, checked our SaaS Databases for Indicators of Compromise, and have had external security experts review our code to ensure a successful service restart.

SaaS Restoration Timeline Updates

- Our executive committee will meet on July 5th at 5:00 AM UTC (12:00 AM EDT) to make a readiness decision on restarting SaaS within the following time windows:
  - EU, UK, & APAC Data Centers: July 5 – 9:00 AM UTC – 1:00 PM UTC (4:00 AM EDT – 8:00 AM EDT)
  - North American Data Centers: July 5 – 5:00 PM EDT – 10:00 PM EDT
- These times/dates are subject to change and a status update will be posted on the website by 1:00 AM UTC as to whether we are adhering to the above schedule or not. If not, we will publish a revised schedule at that time.

For our SaaS Users:

- We will bring our SaaS data centers back online on a one-by-one basis starting with our EU, UK and APAC data centers followed by our North American data centers.
- We will be adding an additional layer of security to our SaaS infrastructure which will change the underlying IP addresses of our VSA servers.

For our On-Premises Users

  - We are currently building our on-premises release to make available to customers. We will begin the communication of the on-premises release process on July 5
  - We are working on a program to enable us to extend our new security measures to our on-premises customers. Most details for this will be available prior to the release of the on-premises patch.

Continued Advisory

- 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 security posture.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links – they may be weaponized.**
- The new Compromise Detection Tool can be download at the following link: VSA Detection Tools.zip | Powered by Box This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.

July 4, 2021 - 10:00 AM EDT

Next Update will be published July 4th in the early afternoon EDT

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.
This update provides further detail on the 1:30 PM EDT update. The changes are underlined for clarity.

Our security, support communications, and customer teams continue to work around the clock in all geographies through the weekend to resolve the issue and restore our customers to service.

This update provides further detail on the July 3, 2021 7:30 PM EDT and 9:00 PM EDT updates. The changes are underlined for clarity.

Continued Advisory

- Hosted VSA Servers will become operational once Kaseya has determined that we can safely restore operations. We are in the process of formulating a staged return to service of our SaaS server farms with restricted functionality and a higher security posture (estimated in the next 24-48 hours but that is subject to change) on a geographic basis. More details on both the limitations, security posture changes, and time frame will be in the next communique later today.
- 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 security posture.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links as they may be weaponized.**

Key Points on Current Status

- The new Compromise Detection Tool was rolled out last night to almost 900 customers who requested the tool. Based on feedback from customers, we will be publishing an update to the tool this morning that improves its performance and usability. **There are no changes that will require a re-run of the tool on systems that have been scanned.**
  This new version of the Compromise Detection Tool will be automatically sent to customers who received the first version. New requests can be made by sending an email to [email protected] with the subject “Compromise Detection Tool Request”.
- We will be opening up a private download site for end customers to get access to the Compromise Detection Tool once we have ensured the security, integrity, and trackability of the download process. More about this in the next update.
- We continue to work with FireEye Mandiant IR (a leading computer incident response firm) on the security incident. Our joint efforts have not identified any new IoCs since yesterday and we have deployed our Compromise Detection Tool at hundreds of customers. At this point, no “False Positives” have been reported by users. [Note: A “False Positive” indicates that the Compromise Detection Tool incorrectly classifies a system as impacted when it wasn’t]
- We have been actively engaged with FireEye and other security assessment firms to assess the manner and impact of the attack to ensure that our R&D organization has properly identified and mitigated the vulnerability. We are continuing the investigation in parallel with the remediation steps.
- R&D has replicated the attack vector and the mitigation work is in progress. We expect to complete the work in the next 24-48 hours and the testing is progressing in parallel.

- Fred Voccola, CEO of Kaseya, was interviewed regarding this incident on Good Morning America on the ABC network on Sunday, July 4th. The interview was significantly edited down from the full interview that Fred gave. The short message was: “We are sure we know how it happened and we are remediating it.”
- We have engaged with the FBI and DHS CISA and are working with them on an incident-handling process for our worldwide customers impacted by the cyberattack. The following message will be posted to the FBI website:
  ““If you feel your systems have been compromised as a result of the Kaseya ransomware incident, we encourage you to employ all recommended mitigations, follow Kaseya’s guidance to shut down your VSA servers immediately, and report your compromise to the FBI at https://www.IC3.gov. Due to the potential scale of this incident, we may be unable to respond to each victim individually but all information we receive will be useful in countering this threat.”
- At this time, we believe that none of our NOC customers (neither SaaS nor on-premises) were affected by the attack. We’re continuing to investigate, but no compromised NOC customers have been found as of July 4th at 10:00 AM EDT.
- Kaseya executives are directly reaching out to impacted customers to understand their situations and what assistance is possible. If you believe that you have been impacted, please contact [email protected] with the subject “Security Incident Report.” **There have been no new reports of compromises since our last report yesterday.** We are confident we understand the scope of the issue and are partnering with each client to do everything possible to remediate. We believe that there is zero related risk right now for any VSA client who is a SaaS customer or on-premises VSA customer who has their server offline.

July 3, 2021 - 9:00 PM EDT

Kaseya’s VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams’ fast response, we believe that this has been localized to a very small number of on-premises customers only.

This update provides further detail on the 1:30 PM EDT update. The changes are underlined for clarity.

Key Points on Current Status:

- 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. We plan to give our first time estimate in tomorrow morning’s update at approximately 9:00 AM EDT.
- SaaS & Hosted VSA Servers will become operational once Kaseya has determined that we can safely restore operations.

- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links, as they may be weaponized.**
- A Compromise Detection Tool will be available **later this evening** to Kaseya VSA customers by sending an email to [email protected] with the subject “Compromise Detection Tool Request” from an email address that is associated with a VSA customer.
- With the availability of the Compromise Detection tool, we strongly recommend that compromised customers immediately begin the recovery process.
- Fred Voccola, CEO of Kaseya, will be interviewed regarding this incident on Good Morning America on the ABC network on Sunday, July 4th. Please consult your local TV listings for times in your region. (This is subject to last minute rescheduling by the network)
- Kaseya executives are directly reaching out to impacted customers to understand their situations and what assistance is possible. If you believe that you have been impacted, please contact [email protected] with the subject “Security Incident Report.” There has been only one new report of a compromise occurring today due to a VSA on-premises server being left on. We are confident we understand the scope of the issue and are partnering with each client to do everything possible to remediate. We believe that there is zero related risk right now for any VSA client who is a SaaS customer or on-prem VSA customer who has their server off.
- We have engaged a computer incident response firm (FireEye Mandiant IR) to identify the indicators of compromise (IoCs) to ensure that we can identify which systems and data were accessed. We have identified a set of preliminary IoCs and have been working with our affected customers to validate them. The availability of the Compromise Detection Tool is based on our interactions with our outside experts.
- We have been actively engaged with FireEye and other security assessment firms to assess the manner and impact of the attack to ensure that our R&D organization has properly identified and mitigated the vulnerability.
- R&D has replicated the attack vector and is working on mitigating it. We have begun the process of remediating the code and will include regular status updates on our progress starting tomorrow morning. We will begin working with select customers to field test the changes once we have completed the work and tested it thoroughly in our environment. We will not publish a resolution timeframe until we have thoroughly validated and tested the proposed solution.
- At this time, we believe that none of our NOC customers (neither SaaS nor on-premises) were affected by the attack. We’re continuing to investigate this, but no compromised NOC customers have been found as of 7:00 PM EDT.
- We have engaged with the FBI and are working with them on an incident-handling process for our worldwide customers impacted by the cyberattack.

July 3, 2021 - 1:30 PM EDT

Kaseya is progressing on the security incident along multiple workstreams:

- Since the security of our customers is paramount, **we are continuing to strongly recommend that our on-premises customers' VSA servers remain offline until further notice.** We will also keep our SaaS servers offline until further notice.
- **We have been advised by our outside experts, that customers who experienced ransomware and receive communication from the attackers should not click on any links — they may be weaponized.**
- We have engaged with the FBI and are working with them on an incident handling process for our worldwide customers impacted by the cyberattack. We will be publishing a list of contacts later today.
- Kaseya executives are directly reaching out to impacted customers to understand their situations and what assistance is possible. Anyone who believes they have been impacted should contact [email protected] with the subject "Security Incident Report."
- We continue to engage with industry experts to assess the manner and impact of the attack and ensure that our R&D organization has properly identified and mitigated the vulnerability.
- R&D has replicated the attack vector and is working on mitigating it. We will not publish a resolution timeframe until we have thoroughly validated and tested the proposed solution. We appreciate our customers' patience.
- We have engaged a computer forensics firm to identify the indicators of compromise (IOCs) to ensure that we can identify which systems and data were accessed.
- R&D is working on a self-assessment tool for our customers, to enable them to definitively determine whether they were affected. This will be published as part of the patch for on-premises customers.

At this time, we believe that none of our NOC customers (neither SaaS nor on-premises) were affected by the attack. We're continuing to investigate this.

- **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.**
- **SAAS & HOSTED VSA SERVERS WILL BECOME OPERATIONAL ONCE KASEYA HAS DETERMINED THAT WE CAN SAFELY RESTORE OPERATIONS.**

July 3, 2021 - 10:30 AM EDT

Kaseya's VSA product has unfortunately been the victim of a sophisticated cyberattack. Due to our teams' fast response, we believe that this has been localized to a very small number of on-premises customers only.

Since the security of our customers is paramount, **we are continuing to strongly recommend that our on-premises customers' VSA servers remain down until further notice.** We will also keep our SaaS servers offline until further notice.

We have been advised by our outside experts, that customers who experienced ransomware and receive a communication from the attackers should not click on any links – they may be weaponized.

Kaseya has been working around the clock to resolve this issue from a security assessment, client support, progress update, technical resolution, and return to operational status standpoint.

A comprehensive update is in progress and will be published later this morning (EDT). This communication will include prescriptive information on:

- The external authorities (FBI, Incident Response Experts) that we have engaged and how we are leveraging them for assistance;
- How our customers can engage Kaseya for assistance and what we can do to help;
- How to determine whether customers have been compromised;
- Status updates from R&D on the progress of the patch for on-premises users;
- The plan to bring our SaaS and on-premises customers back online;
- A detailed description of the Security Incident process and current status;
- A schedule for communications updates;
- Other important information about the recovery process.

Ongoing updates will be provided every 3-4 hours or more often based on breaking details.

1. ALL ON-PREMISEs VSA SERVERS SHOULD CONTINUE TO REMAIN OFFLINE UNTIL FURTHER INSTRUCTIONS FROM KASEYA.
2. SAAS & HOSTED VSA SERVERS WILL BECOME OPERATIONAL ONCE KASEYA HAS DETERMINED THAT WE CAN SAFELY RESTORE OPERATIONS.

July 2, 2021 - 10:00 PM EDT

Beginning around mid-day (EDT/US) on Friday July 2, 2021, Kaseya's Incident Response team learned of a potential security incident involving our VSA software.

We took swift actions to protect our customers:

- Immediately shut down our SaaS servers as a precautionary measure, even though we had not received any reports of compromise from any SaaS or hosted customers;
- Immediately notified our on-premises customers via email, in-product notices, and phone to shut down their VSA servers to prevent them from being compromised.

We then followed our established incident response process to determine the scope of the incident and the extent that our customers were affected.

- We engaged our internal incident response team and leading industry experts in forensic investigations to help us determine the root cause of the issue;
- We notified law enforcement and government cybersecurity agencies, including the FBI and CISA.

While our early indicators suggested that only a very small number of on-premises customers were affected, we took a conservative approach in shutting down the SaaS servers to ensure we protected our more than 36,000 customers to the best of our ability. We have received positive feedback from our customers on our rapid and proactive response.

While our investigation is ongoing, to date we believe that:

- Our SaaS customers were never at-risk. We expect to restore service to those customers once we have confirmed that they are not at risk, which we expect will be within the next 24 hours;
- Only a very small percentage of our customers were affected – currently estimated at fewer than 40 worldwide.

We believe that we have identified the source of the vulnerability and are preparing a patch to mitigate it for our on-premises customers that will be tested thoroughly. We will release that patch as quickly as possible to get our customers back up and running.

I am proud to report that our team had a plan in place to jump into action and executed that plan perfectly today. We’ve heard from the vast majority of our customers that they experienced no issues at all, and I am grateful to our internal teams, outside experts, and industry partners who worked alongside of us to quickly bring this to a successful outcome.

Today’s actions are a testament to Kaseya’s unwavering commitment to put our customers first and provide the highest level of support for our products.

Fred Voccola, CEO
Kaseya