Q1 2018 VSA Security Update

Update - February 16, 2018

As part of Kaseya's efforts to improve our products, adapt to the evolving cyber-threat landscape, and identify and respond to new threats as they arise – including through invaluable feedback from partners like eSentire – Kaseya continues to harden the security of our software products.

We strongly recommend that all our on-premises VSA customers immediately download and install these patches to further harden the VSA product's security. These updates have already been deployed to our SaaS and hosted VSA environments.

Although we have no indication of widespread access to VSA user names or passwords, in this instance, as with any other vulnerability which may arise with any software you use, such access is possible. As such, we recommend immediately adopting best practices for securing user credentials – including changing passwords regularly or using multi-factor authentication – which can be very helpful to mitigating the impact of any vulnerability.

In order to determine whether you have been affected, Kaseya recommends customers run a set of Agent Procedures across their environment. Technical details, the procedure and detailed instructions are located at the following link: https://helpdesk.kaseya.com/hc/en-gb/articles/360000346651.

Today's and future patches will continue to improve security, as well as functional improvements and bug fixes to the VSA. We and our security partners will continue monitoring the situation and we will issue additional patches as necessary to ensure that the product remains secure in the face of any evolving threats.

As always, Kaseya Support is available to assist customers and can be reached by submitting a request at https://helpdesk.kaseya.com/hc/en-gb/requests/new and selecting "VSA Security" under Module to ensure your question is properly routed.

Patch Information

On-Premise VSA Customers – Kaseya strongly recommends that on-premises customers immediately apply a patch by running the Kinstall (Kinstall.exe) that is included on the VSA server: (that matches the version of VSA that you are running):

Version R9.5: Patch 9.5.0.5

Version R9.4: Patch 9.4.0.36

Version R9.3: Patch 9.3.0.35

For customers running Version R9.2 or earlier, it is recommended to upgrade to 9.3 or higher. If needed, Kaseya support can assist you with this. Please reach out to Kaseya Support by submitting a request at https://helpdesk.kaseya.com/hc/en-gb/requests/new and selecting "VSA Security" under Module to ensure your question is properly routed.

SaaS or Hosted Customers - The updates have been applied by Kaseya, no action is required.

Kaseya is committed to quality and security in our products and maintaining transparency in our communications with our customer base.

January 28, 2018 - Original Post Below

In the course of our continuous security monitoring of our products, we have uncovered a security vulnerability in our VSA product.

Consistent with our commitment to providing secure solutions for our partners, we have issued a set of patches that removes this vulnerability. We strongly recommend that every on-premises VSA customer download and install this patch immediately. The patch to address this vulnerability has already been deployed to our SaaS and hosted servers.

We have seen no evidence to suggest that this vulnerability was used to harvest personal, financial, or other sensitive information. However, we are aware of a small subset of our partners where Monero cryptocurrency mining software was deployed to endpoints. Our initial estimates indicate that less than 0.1% of our customers have been affected by this issue.

Kaseya Support is available to assist customers and can be reached by submitting a request at https://helpdesk.kaseya.com/hc/en-gb/requests/new and selecting "VSA Security" under Module to ensure your question is properly routed.

Patch Information

On-Premise VSA Customers – Kaseya strongly recommends that on-premises customers immediately apply a patch by running the Kinstall (Kinstall.exe) that is included on the VSA server: (that matches the version of VSA that you are running):

Version R9.5: Patch 9.5.0.3

Version R9.4: Patch 9.4.0.35

Version R9.3: Patch 9.3.0.34

For customers running Version R9.2 or earlier, it is recommended to upgrade to 9.3 or higher. If needed, Kaseya support can assist you with this. Please reach out to Kaseya Support by submitting a request at

https://helpdesk.kaseya.com/hc/en-gb/requests/new and selecting “VSA Security” under Module to ensure your question is properly routed.

SaaS or Hosted Customers - The updates have been applied by Kaseya, no action is required.

Kaseya is committed to quality and security in our products and maintaining transparency in our communications with our customer base.

Assessment & Remediation

To provide further assurances, Kaseya has created Agent Procedures which customers can run across their environment to determine if they were affected by this vulnerability and remediate endpoints in the event they were impacted. The procedure and detailed technical instructions are located at the following link: https://helpdesk.kaseya.com/hc/en-gb/articles/360000346651

Kaseya is committed to quality and security in our products and maintaining transparency in our communications with our customer base.

Browse this section