Sisense Log4j Vulnerability Updates

Update - December 23, 2021

Statement on additional log4j vulnerability and remediation path

Sisense Security and Development teams have updated the impacted libraries of log4j to version 2.16 on our current and past releases given the critical nature and immediate threat of these exploits (CVE-2021-45046 || CVE-2021-44228). Sisense followed guidance provided by both CISA and Apache.

The additional high severity log4j exploit (CVE-2021-45105) which poses a potential for DoS attacks requires an update to log4j version 2.17. This new version is implemented as part of our upcoming Sisense release 2021.12 in accordance with our vulnerability management process. Additionally, this aligns with our remediation timelines per our Information Security policies. As previously mentioned, we have also implemented measures for our cloud customers to mitigate the risk of the CVE-2021-45105 exploit (DoS attacks) using controls available to us through our partner CloudFlare. For on-premises customers, and customers that are running on the Sisense cloud, but controlling their own DNS, we recommend using CloudFlare with Log4j rules or any other WAF as an additional measure to address this lower severity exploit.

Sisense is continuing efforts to implement measures to protect against the log4j vulnerability and has released additional hotfixes for older Linux versions as well as an update to the Windows patch.

The newly released hotfixes are as follows:

- Linux L2021.3.0
- Linux L2021.3.2
- Linux L2021.5.0
- Linux L2021.9.0
- Linux L2021.8.0
- Linux L2021.1.4
- Windows patch update (Dec 22nd)

Our customers running on the Sisense Cloud were protected immediately by hardening our firewall. At this time, we have completed all patches for Cloud customers for this vulnerability.

For our Windows on-premise customers, the updated patch includes extra validation and scanning for other directories where related files may exist. We advise our customers to rerun the patch per the Windows Patch instructions located here: Windows On-Prem Patch Instructions.

Our customers running Sisense on-premise, please see the next page for download links to released hotfixes. Linux hotfixes are run as an “upgrade in place” to the same version you are currently using. Please refer to this Help Documentation for instructions: Upgrading Sisense for Linux.

Release L2021.1

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.1.4.126-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.1.4.126-DockerHub-offline-installer.tar.gz

Release L2021.3.0:

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.3.0.253-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.3.0.253-DockerHub-offline-installer.tar.gz

Release Linux L2021.3.2:

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.3.2.87-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.3.2.87-DockerHub-offline-installer.tar.gz

Release Linux L2021.5.0

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.5.0.282-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.5.0.282-DockerHub-offline-installer.tar.gz

Release Linux L2021.9.0

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.9.0.61-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.9.0.61-DockerHub-offline-installer.tar.gz

Release Linux L2021.8.0

Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.8.0.99-DockerHub.tar.gz

Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.8.0.99-DockerHub-offline-installer.tar.gz

Release Linux L2021.1.4
Direct link URL: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.1.4.126-DockerHub.tar.gz
Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.1.4.126-DockerHub-offline-installer.tar.gz

Windows (Updated Dec 23, 2021)
Instructions:
https://cloudops-sisense.s3.us-east-2.amazonaws.com/fix_log4j_Sisense.zip

Please reach out to your CSM or go to support.sisense.com to submit a support ticket for any further questions or concerns.

Update - December 16, 2021

Sisense is actively working on implementing measures to protect against exploitation of our product and have issued a hotfix for the following releases:

- Linux 2021.10
- Linux 2021.11
- Patch for all Windows versions

Our customers running on the Sisense Cloud were protected immediately by hardening our firewall. We are actively working on patching them with minimal to no downtime.

Our customers who are running Sisense on-premise, please refer below for download instructions:

Release 2021.11:

Direct Link: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.11.0.127-DockerHub.tar.gz
Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.11.0.127-DockerHub-offline-installer.tar.gz

Release 2021.10

Direct Link: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.10.0.158-DockerHub.tar.gz
Offline: https://data.sisense.com/linux/sisense_kubespray_deployment-L2021.10.0.158-DockerHub-offline-installer.tar.gz

Windows

Windows On-Prem Patch Instructions
Direct Link: https://cloudops-sisense.s3.us-east-2.amazonaws.com/fix_log4j_Sisense.zip

Update - December 15, 2021

Sisense Windows Patch for Log4j Vulnerability (Updated 12/23/21)

Link: https://cloudops-sisense.s3.us-east-2.amazonaws.com/fix_log4j_Sisense.zip

We have relocated the Windows Patch instructions to its own file located here: Windows On-Prem Patch Instructions

Update - December 14, 2021

This patch will fix Sisense log4j vulnerability in Connectors and Shipper. It applies only for native out of the box Sisense Windows:

Link: https://cloudops-sisense.s3.us-east-2.amazonaws.com/fix_log4j_Sisense.zip

1. Extract the zip file into C:\Scripts\ the structure should be once unzipped C:\Scripts\fix_log4j

2. Run as Admin the PowerShell file C:\Scripts\fix_log4j\fixLog4jSisense.ps1

3. Review the logs under C:\Scripts\fix_log4j\log.txt and make sure there are no errors, in case there are ERRORs please consult with the Sisense support team.

Update - December 13, 2021

Sisense Update on Log4j Vulnerability

Over this past weekend, a critical vulnerability was identified in a commonly used java library named log4j. This 3rd party library is used within the Sisense application and may introduce the potential for it to be exploited under specific circumstances. Sisense has prepared the following recommended guidance for our customers:

- In Sisense products, the vulnerability can only be exploited by an authenticated and named user that has the proper privileges. No attack vectors are open from outside the application.
- If you are running on the standard Sisense managed cloud, the vulnerability has already been resolved by Sisense and requires no further action.
- For on premises customers and customers that are running on the Sisense cloud, but controlling their own DNS, we recommend using CloudFlare with Log4j rules or any WAF. Customers will need to create a rule (if it is not provided by the vendor) to block requests that contain in request header/body/URI query parameters “{jndi:”.
    - Note that after this change, Windows customers will not have access to RDWEB temporarily until the formal patch is released. To access FTP, customers should reach out to Customer Support to get the IP for the FTP connection.
- For customers that cannot implement a WAF service there are manual steps that can be taken to remove the use of log4j from your instance. Please go to support.sisense.com for assistance.