Security Vulnerability
Released: December 12, 2021
Last updated: December 13, 2021
Assigning CNA: Apache Software Foundation

Security Advisory Summary

UPDATE December 13, 2021: NOTE:
This security vulnerability only affects Server & Application Monitor (SAM) and Database Performance Analyzer (DPA) and does not affect any other SolarWinds or N-able (formerly SolarWinds MSP) products.

You can Subscribe to this RSS feed to be notified when we update this page (note: you will need to cut and paste the "Subscribe to this RSS feed" URL into an RSS Feed Reader, e.g., Outlook’s RSS Subscriptions, to monitor updates).

December 9, 2021, the Apache Software Foundation released Log4j 2.15.0 to resolve a critical remote code execution vulnerability (CVE-2021-44228) affecting versions 2.0-beta9 through 2.14.1.

Apache Log4j is a popular Java logging library incorporated into a wide range of enterprise software (including Struts2, Solr, Druid, and Flink). This is a well-known vulnerability affecting numerous software companies.

The following SolarWinds products utilize an affected version of Apache Log4j in their codebase:

- Server & Application Monitor (SAM)
- Database Performance Analyzer (DPA)

First, it’s important to note the Orion Platform core is not affected and does not utilize Apache Log4j. The only two SolarWinds products we have identified as affected by this vulnerability are Server & Application Monitor (SAM) and Database Performance Analyzer (DPA). We have not identified any other SolarWinds products as affected by this vulnerability.

Server & Application Monitor (SAM) (JMX Monitoring feature) utilizes the vulnerable Log4j library, but it uses the JDK version 16 which is not known at this time to be susceptible to the Log4j vulnerability. In an abundance of caution, SolarWinds
engineers are producing a hotfix to replace the existing library with the latest version. This hotfix is being planned and the release schedule will be updated soon. Please refer to this page for updates.

Suggested workaround steps prior to hotfix availability can be found in the following KB Article: https://support.solarwinds.com/SuccessCenter/s/article/Server-Application-Monitor-SAM-and-the-Apache-Log4j-Vulnerability-CVE-2021-44228?language=en_US

This workaround is targeted for customers running SAM 2020.2.6 and later, as earlier versions of SAM are based on an older version of Log4j unaffected by this issue. You can check your version by looking into folder: Orion-Installation\APM\jmxbridge.

**Database Performance Analyzer (DPA)** utilizes the vulnerable library but also uses a later version of the Java SDK which may reduce the risk of the vulnerability. SolarWinds engineers are producing a hotfix to replace the existing library with the latest version. This hotfix is being planned and the release schedule will be updated soon. Please refer to this page for updates.

Prior to hotfix’s availability, the Log4j libraries can be replaced manually on Windows by following the steps in the following kB article: https://support.solarwinds.com/SuccessCenter/s/article/Database-Performance-Analyzer-DPA-and-the-Apache-Log4j-Vulnerability-CVE-2021-44228?language=en_US

This workaround is targeted for customers running the following versions, as earlier versions of DPA are based on an older version of Log4j unaffected by this issue.

- 2021.1.x
- 2021.3.x
- 2022.1.x

The Linux instructions for DPA are in the process of being validated and will be provided once they are confirmed.

If an upgrade is not possible at this time, to help mitigate the risk to your DPA installation, please ensure your environment is appropriately configured and utilizes the DPA Secure Configuration Guide: Best Practices and Recommendations, available at: https://support.solarwinds.com/SuccessCenter/s/article/DPA-Secure-Configuration-Guide-Best-Practices-and-Recommendations

**FAQ**

**What happened?** December 9, 2021, the Apache Software Foundation released Log4j 2.15.0 to resolve a critical remote code execution vulnerability (CVE-2021-44228) affecting versions 2.0-beta9 through 2.14.1.

Log4j is a popular Java logging library incorporated into a wide range of Apache enterprise software (including Struts2, Solr, Druid, and Flink).
Why am I seeing so much about this in the media? This is a well-known vulnerability, affecting numerous software companies.

Have there been any reports to SolarWinds? While there have not been any user or security researcher reports of this vulnerability affecting SolarWinds software, we have received several customer inquiries, given the broad industry usage of Apache software and recent media coverage.

How is SolarWinds addressing this? Our investigations of this issue are active and ongoing. This update is as of Monday, December 13, 2021, at 4:00 p.m. CT. The Orion Platform core is not affected and does not utilize Apache Log4j.

What SolarWinds products are affected? The following SolarWinds products utilize an affected version of Apache Log4j in their codebase:

- Server & Application Monitor (SAM)
- Database Performance Analyzer (DPA)

We have not identified any other SolarWinds products as affected by this vulnerability.

What do I need to know about SAM? Server & Application Monitor (SAM) (JMX Monitoring feature) utilizes the vulnerable Log4j library, but it uses JDK version 16 which is not known at this time to be susceptible to the Log4j vulnerability. In an abundance of caution, SolarWinds engineers are producing a hotfix to replace the existing Apache library with the latest version. This hotfix is being planned and the release schedule will be updated soon.

What do I need to know about DPA? Database Performance Analyzer (DPA) utilizes the vulnerable library but also uses a later version of the Java SDK which may reduce the risk of the vulnerability. SolarWinds engineers are producing a hotfix to replace the existing library with the latest version. This hotfix is being planned and the release schedule will be updated soon. Prior to hotfix’s availability, the Log4j libraries can be replaced manually on Windows by:

- Download the latest version of Log4j
- Stopping the Windows Service “Ignite PI Server”
- Backing up then replacing the following files
  - log4j-api-2.xx.y.jar
  - log4j-core-2.xx.y.jar
  - log4j-slf4j-impl-2.xx.y.jar
- Restart DPA and the “Ignite PI Server”

The Linux instructions for DPA are in the process of being validated and will be provided once they are confirmed.

If an upgrade is not possible, to help mitigate the risk to your DPA installation, please ensure your environment is appropriately configured and utilizes the DPA Secure Configuration Guide: Best Practices and Recommendations, available
What actions should I take? SolarWinds recommends its customers upgrade to the latest versions of these products once they become generally available. SolarWinds also always recommends implementing the safeguards in the Secure Configuration for the Orion Platform guide available at: https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-secure-configuration.htm

Is the Orion Platform code affected? No, the Orion Platform core is not affected and does not utilize Apache Log4j.


Disclaimer
Please note, any content posted herein is provided as a suggestion or recommendation to you for your internal use. This is not part of the SolarWinds software or documentation that you purchased from SolarWinds, and the information set forth herein may come from third parties. Your organization should internally review and assess to what extent, if any, such custom scripts or recommendations will be incorporated into your environment. You elect to use third-party content at your own risk, and you will be solely responsible for the incorporation of the same if any.

Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>December 13, 2021</td>
<td>Updated FAQ information. Added RSS feed instructions. These are informational changes only.</td>
</tr>
<tr>
<td>1.2</td>
<td>December 12, 2021</td>
<td>Added KB article links. This is an informational change only.</td>
</tr>
<tr>
<td>1.1</td>
<td>December 12, 2021</td>
<td>Updated FAQ information. This is an informational change only.</td>
</tr>
<tr>
<td>1.0</td>
<td>December 12, 2021</td>
<td>Information Published</td>
</tr>
</tbody>
</table>