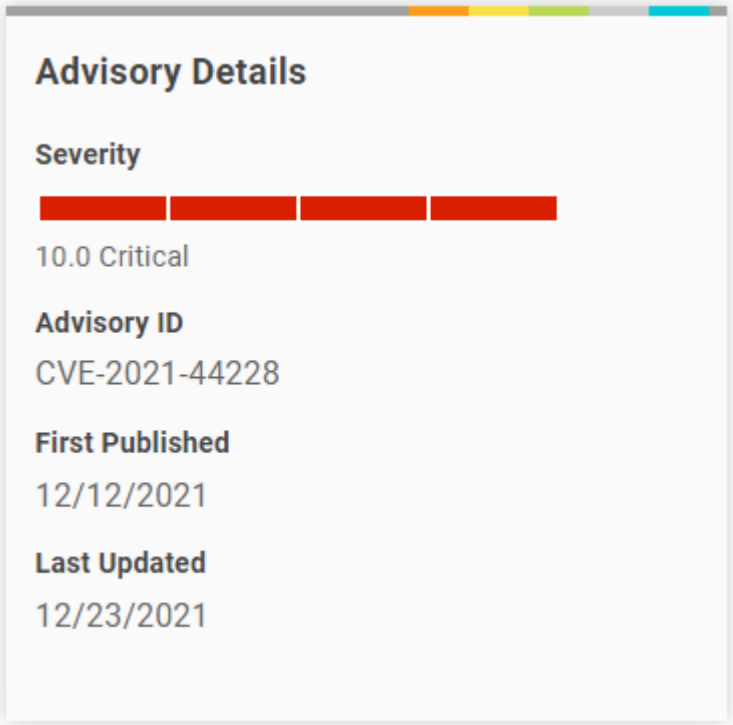
Security Vulnerability

Released: December 12, 2021 Last updated: December 23, 2021
Assigning CNA: Apache Software Foundation

Security Advisory Summary

UPDATE December 23, 2021: Updated to announce the availability of the Database Performance Analyzer (DPA) hotfix released December 22, 2021, which is available for DPA customers in their Customer Portal



at https://customerportal.solarwinds.com/. Additionally, NIST has upgraded the severity of CVE-2021-45046 from 3.7 Low to 9.0 Critical. We've also added new CISA mitigation guidance: *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities.*

SolarWinds recommends customers of SAM and DPA apply the available hotfixes to their systems, and follow the guidance captured in the accompanying release notes.

UPDATE December 20, 2021: Updated to announce the availability of the Server & Application Monitor (SAM) hotfix released today, December 20, 2021, which is available for SAM customers in their Customer Portal at https://customerportal.solarwinds.com/.

UPDATE December 18, 2021: SolarWinds is evaluating the Apache Log4j Denial of Service vulnerability CVE-2021-45105, announced December 18, 2021, and the release of Apache Log4j 2.17. Please visit this page for updates. 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).

UPDATE December 17, 2021: Updated to announce the availability of the Database Performance Analyzer (DPA) hotfix released today, December 17, 2021, which is available for DPA customers in their Customer Portal at https://customerportal.solarwinds.com/.

This update also reflects CISA Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability, issued December 17, 2021, and we have posted a new security advisory for CVE-2021-4104.

Guidance for all three CVEs related to the Log4j issue is available on this page:

- CVE-2021-44228
- CVE-2021-45046
- CVE-2021-4104

UPDATE December 16, 2021: Updated to reflect availability of and support for Log4j 2.16.0 to resolve CVE-2021-45046 vulnerability reported on Log4j.

NOTE: SolarWinds products do not use JMSAppender, and are not known to be affected by the vulnerability identified in CVE-2021-4104.

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.

December 13, 2021, the Apache Software Foundation released Log4j 2.16.0 to disable default access to JNDI lookups and limits the protocols by default to only java, ldap, and ldaps and limits the ldap protocols to only accessing Java primitive objects to resolve a vulnerability which could leave an affected system open to a Denial-of-Service (DOS) attack (CVE-2021-45046).

December 17, 2021, the Apache Software Foundation released Log4j 2.17.0 to resolve a Denial-of-Service vulnerability in Apache Log4j2 versions 2.0-alpha1 through 2.16.0, which did not protect from uncontrolled recursion from self-referential lookups (CVE-2021-45105).

December 21, 2021, the National Institute of Standards and Technology (NIST) upgraded CVE-2021-45046 from a severity of 3.7 (Low) as originally reported on December 14, to 9.0 (Critical).

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) in versions prior to the recent hotfixes utilize 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. SolarWinds recommends upgrading your version of SAM to the latest available, or following the instructions provided in the KB article linked below to update the Log4j libraries it uses, for the protection of your environment.

SolarWinds engineers released a hotfix December 20, 2021, to replace the existing library with Apache Log4j 2.16.0. You can download the hotfix for your SAM version in your Customer Portal at https://customerportal.solarwinds.com.

For more information, please see the following KB article for the latest details specific to the SAM hotfix: https://support.solarwinds.com/SuccessCenter/s/article/Server-Application-Monitor-SAM-and-the-Apache-Log4j-Vulnerability-CVE-2021-44228?language=en_US.

As the Apache Software Foundation continues to update Log4j, SolarWinds will examine compatibility with SAM and will update this article accordingly.

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 recommends upgrading your version of DPA to the latest available, or following the instructions provided in the KB article linked below to update the Log4j libraries it uses, for the protection of your environment.

SolarWinds engineers released a hotfix December 22, 2021, to replace the existing library with Apache Log4j 2.17.0. You can download the hotfix for your DPA version in your Customer Portal at https://customerportal.solarwinds.com.

For more information, please see 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. As the Apache Software Foundation continues to update Log4j, SolarWinds will examine compatibility with DPA and will update this article accordingly.

This issue affects DPA customers running the following versions, as earlier versions of DPA are based on an older version of Log4j without this issue:

- DPA 2021.1.x
- DPA 2021.3.x

- DPA 2022.1 RC1

As a best practice, SolarWinds always recommends you 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.

December 13, 2021, the Apache Software Foundation released Log4j 2.16.0 to disable default access to JNDI lookups and limits the protocols by default to only Java, LDAP, and LDAPS and limits the LDAP protocols to only accessing Java primitive objects to resolve a vulnerability which could leave an affected system open to a Denial-of-Service (DOS) attack (CVE-2021-45046).

December 17, 2021, the Apache Software Foundation released Log4j 2.17.0 to resolve a Denial-of-Service vulnerability in Apache Log4j2 versions 2.0-alpha1 through 2.16.0, which did not protect from uncontrolled recursion from self-referential lookups (CVE-2021-45105).

December 21, 2021, the National Institute of Standards and Technology (NIST) upgraded CVE-2021-45026 from a severity of 3.7 (Low) as originally reported on December 14, to 9.0 (Critical).

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. The Apache Software Foundation's resolution process is fluid, and as they release later versions of Log4j, we will support those versions, and will provide updates accordingly.

This update is as of Thursday, December 23, 2021, at 7:00 a.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.

SolarWinds engineers released a hotfix December 20, 2021, to replace the existing library with Apache Log4j 2.16.0. You can download the hotfix for your SAM version in your Customer Portal at https://customerportal.solarwinds.com.

For more information, please see the following KB article for the latest details specific to the SAM hotfix: https://support.solarwinds.com/SuccessCenter/s/article/Server-Application-Monitor-SAM-and-the-Apache-Log4j-Vulnerability-CVE-2021-44228?language=en_US. As the Apache Software Foundation continues to update Log4j, SolarWinds will examine compatibility with SAM and will update this article accordingly.

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 released a hotfix December 22, 2021, to replace the existing library with Apache Log4j 2.17.0. You can download the hotfix for your DPA version in your Customer Portal at https://customerportal.solarwinds.com/.

For more information, please see 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. As the Apache Software Foundation continues to update Log4j, SolarWinds will examine compatibility with DPA and will update this article accordingly.

This issue affects DPA customers running the following versions, as earlier versions of DPA are based on an older version of Log4j without this issue:

- DPA 2021.1.x
- DPA 2021.3.x
- DPA 2022.1 RC1

As a best practice, SolarWinds always recommends you 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.

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.

I've heard about a new vulnerability with JMSAppender – is SolarWinds affected by this vulnerability? SolarWinds products do not use JMSAppender, and are not known to be affected by the vulnerability identified in CVE-2021-4104.

Is there any additional information available? Please refer to following resources:

Cybersecurity & Infrastructure Security Agency (CISA) guidance:

- *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (published December 22, 2021): https://www.cisa.gov/uscert/ncas/current-activity/2021/12/22/mitigating-log4shell-and-other-log4j-related-vulnerabilities*
- *Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability (issued December 17, 2021): https://www.cisa.gov/emergency-directive-22-02*
- *CISA Issues ED 22-02 Directing Federal Agencies to Mitigate Apache Log4j Vulnerabilities (published December 17, 2021): https://www.cisa.gov/uscert/ncas/current-activity/2021/12/17/cisa-issues-ed-22-02-directing-federal-agencies-mitigate-apache*
- *Apache Log4j Vulnerability Guidance* page (published December 15, 2021): https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- *CISA Log4j (CVE-2021-44228) Vulnerability Guidance GitHub repository* (created December 14, 2021): https://github.com/cisagov/log4j-affected-db
- *Statement from CISA Director Easterly on "Log4j" Vulnerability* (published December 11, 2021): https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability
- *Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation* (published December 10, 2021): https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce

The Apache Foundation guidance:

- *Apache Log4j Security Vulnerabilities*: https://logging.apache.org/log4j/2.x/security.html

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

Version	Revision Date	Description
1.8	December 23, 2021	Updated with Database Performance Analyzer hotfix, updated FAQ information. These are informational changes only.
1.7	December 20, 2021	Updated with Server & Application Monitor hotfix, updated FAQ information. These are informational changes only.
1.6	December 18, 2021	Updated FAQ information. These are informational changes only.
1.5	December 17, 2021	Updated with Database Performance Analyzer hotfix, new CISA Emergency Directive 22-02, new SolarWinds security advisory for CVE-2021-4104.
1.4	December 16, 2021	Notice added. Updated FAQ information. These are informational changes only.
1.3	December 13, 2021	Updated FAQ information. Added RSS feed instructions. These are informational changes only.
1.2	December 12, 2021	Added KB article links. This is an informational change only.
1.1	December 12, 2021	Updated FAQ information. This is an informational change only.
1.0	December 12, 2021	Information Published