Important information regarding Apache Log4j library and other security vulnerabilities

12 August 2022

Inhalt

Initial response 13.12.2021 – CVE-2021-44228 - action required

1.1 Affected products: Solr server and tts performance suite 2021r2 server

1.2 Description

tts wants to inform you about the recently disclosed security vulnerability to the open-source **Apache Log4j2 library** (CVE-2021-44228).
We are actively monitoring this problem, and are working on addressing it for all environments running on our cloud infrastructure (SaaS and Managed Hosting) as well as on-premise installations.

1.3 Resolution

Please note the following comments and mitigations for **on-premise installations**:

- tts performance suite uses Log4j2 since **Release 2021 R2**. Therefore, we strongly recommend customers running Release 2021 R2 on premise to add the following JVM arguments or the log4j2 property to close the vulnerability:
  - JVM argument: add "**-Dlog4j2.formatMsgNoLookups=true**"
  - Log4j2 property: add "**log4j2.formatMsgNoLookups=True**"

In case **Solr version 7.4.0 to 7.7.3, 8.0.0 to 8.11.0** is running within the ttsps environment as separate web-application **(no matter what ttps version is currently in use!)**, please add the following to prevent the vulnerability for Solr:

- Linux/MacOS: Edit your **solr.in.sh** file to include:
  SOLR_OPTS="$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"
- Windows: Edit your **solr.in.cmd** file to include:
  set SOLR_OPTS=%SOLR_OPTS% -Dlog4j2.formatMsgNoLookups=true

Further mitigations to close the vulnerability of Solr can be found here:
https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228

1.4 Further information – Cloud customers

For all **SaaS and Managed Hosting** instances tts has taken the recommended and additional actions to ensure the integrity of the services – **no action on your part is required**. Please find a detailed list of actions taken below:

- All tts Cloud environments run behind a Web Application Firewall (WAF). A new rule has been activated on Friday afternoon (5pm GMT) on all WAF instances to block

malicious requests trying to take advantage of this vulnerability. Since then, we observe approximately 80 to 100 intrusion attempts of this nature per hour, however all of these attempts have been blocked successfully. None of the allowed requests contain the attack pattern as described in CVE-2021-44228.

- Our load balancers are not affected and are configured in such a way that requests which are not part of our applications (i.e. paths like */curator*, */webaccess*, */workbench* or */publisher*) are ignored and served with a 404 page directly from the load balancer. They are not forwarded to our Java-based application servers. All recorded intrusion attempts don't use our application paths and would have been ignored by the load balancer.

- Additionally our load balancers only forward requests containing a valid Host-header with the correct hostname (e.g. "customer.tts-cloud.com"). All other requests including only the IP address in the Host-header are ignored. This was the case for all intrusion attempts.

- Since we value the privacy of our customers, we have not activated any access logs per default (not on the application server nor at our load balancers). Since this vulnerability only manifests, if the Log4j2 logging library is configured in such a way that it logs information about a request (URI, User-Agent or any other HTTP header), we are sure that no malicious code has been executed on our servers.

- We also verified all potentially affected customer resources, if an intrusion attempt was successful. However, we did not find any evidence that our servers were compromised. To be sure, we refreshed all potentially affected server with new instances, after the new WAF rule has been activated.

- Over the course of the next days, we will also be rolling out updated versions of the software to tts Cloud and any potentially affected middleware components.

If you have difficulty accessing our service or you observe irregularities in your data, please contact our tts Support immediately.

Having a culture of continuous learning and improvement, we will also take further steps in the coming months to make our tts Cloud environments even safer and provide customers running our software on-premise with additional recommendations on how to strengthen the security of their installations.

Update 15.12.2021 - CVE 2021-44228 - outdated please see chapter 4 for current information

2.1 Affected products: Solr server

2.2 Description

For mitigation of **log4j CVE 2021-44228 in Apache Solr** we recommend to replace the existing log4j libraries with the latest version **2.16.0** (see https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228).
Versions below Solr 7.4 are not affected.

2.3 Resolution

Needed steps to do the update:

1. Stop Solr
2. Go to the following directory and delete the below mentioned libraries
    a. <solrdir>\server\lib\ext
    b. Delete libraries
        i. log4j-1.2-api-2.13.2.jar
        ii. log4j-api-2.13.2.jar
        iii. log4j-core-2.13.2.jar
        iv. log4j-slf4j-impl-2.13.2.jar
        v. log4j-web-2.13.2.jar
    c. Download latest log4j files from https://www.apache.org/dyn/closer.lua/logging/log4j/2.16.0/apache-log4j-2.16.0-bin.zip
    d. Copy following libraries to <solrdir>\server\lib\ext
        i. log4j-1.2-api-2.16.0.jar
        ii. log4j-api-2.16.0.jar
        iii. log4j-core-2.16.0.jar
        iv. log4j-slf4j-impl-2.16.0.jar
        v. log4j-web-2.16.0.jar
    e. Start Solr
    f. Check on Solr Dashboard for any errors> http://<domain>:PORT/solr/

Update 16.12.2021 - CVE-2021-44228 - minor security concern, action recommended

3.1 Affected products: tts performance suite server < 2021r2

Non affected: tts performance suite clients (Producer and QuickAccess) & Solr server

3.2 Description

We would like to issue another update in this matter, as recently addressed by **CVE-2021-44228 Update 4** now also relating to another security vulnerability with **Log4j version 1.x**. See the following link for a complete description: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=9

tts staff have already assessed the possible severity internally. Currently we assume this as **none** to **very low**. This is because we do not normally use the **JMSAppender** and neither do we give out configurations of how to get this setup.

3.3 Resolution

To check yourself if perhaps such an appender has been configured in your environment.

- For this you would have to search within the **application-config.properties** or the **application-config.xml** file (on your local installation of the tts performance suite server) for any active configuration called “jmsappender” and disable or remove such configurations.

Update 20.12.2021 - CVE-2021-45105 - action required

Action required if Chapter 2 has not been applied yet

4.1 Affected products: Solr server 7.4 and higher

4.2 Description

There has been another update to the security vulnerabilities of the Log4J files. Please see this article for further information: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
As with the last update, tts staff have already assessed the possible severity internally. Currently we assume this as **none** to **very low**. This is because we do not use the **context-lookup** in our products and neither does the Solr server.
Versions below Solr 7.4 are not affected.

4.3 Resolution

Necessary steps to do the update:

1. Stop Solr
2. Go to the following directory and delete the below mentioned libraries
    a. <solrdir>\server\lib\ext
    b. Delete libraries
        i. log4j-1.2-api-2.13.2.jar
        ii. log4j-api-2.13.2.jar
        iii. log4j-core-2.13.2.jar
        iv. log4j-slf4j-impl-2.13.2.jar
        v. log4j-web-2.13.2.jar
    c. Download latest log4j files from https://archive.apache.org/dist/logging/log4j/2.17.2/
        i. Direct link for Windows
    d. Copy following libraries to <solrdir>\server\lib\ext
        i. log4j-1.2-api-2.17.2.jar
        ii. log4j-api-2.17.2.jar
        iii. log4j-core-2.17.2.jar
        iv. log4j-slf4j-impl-2.17.2.jar
        v. log4j-web-2.17.2.jar
    e. Start Solr
    f. Check on Solr Dashboard for any errors> http://<domain>:PORT/solr/

Update 25.01.2022 – CVE-2021-44548 – action required

5.1 Affected products: Solr server below 8.11.1

5.2 Description:

The following mitigation concerns customers running any Solr version ***prior to 8.11.1*** in a ***Windows Server***. Customers running a Linux environment or running the latest Solr version (8.11.1) are not affected.

This is a mitigation for **CVE-2021-44548**. More details can be found here: https://nvd.nist.gov/vuln/detail/CVE-2021-44548.

5.3 Resolution

To mitigate this vulnerability, for version of tts performance suite **below (<)** 2021R2 build 104:

- Ensure the DataImportHandler is not being used
  By default this is not enabled for a standard Solr installation **– see below: <Section A>**

  AND

- disable the Config-API
  Add the system property disable.configEdit=true – **see below: <Section B>**

OR if you are running tts performance suite 2021R2 build 104 and higher, then you may choose to update to Solr to 8.11.1, after the update the 2 points above do not apply any-more.

Step by Step for resolution:

<Section A>
Ensure the DataImportHandler is not used

The DataImportHandler would need to be registered in the **solrconfig.xml** file. If the class does not appear, no action is required. If however it is configured, it would look like this (this should then be deactivated or removed immediately):

```
<requestHandler name="/dataimport" class="org.apache.solr.han-
dler.dataimport.DataImportHandler">
  <lst name="defaults">
    <str name="config">/home/username/data-config.xml</str>
  </lst>
</requestHandler>
```

<Section B>
Instructions for disabling the Config API in Solr

The property disable.configEdit=true must be set as a system property. To do this, add -Ddisable.configEdit=true to the start up script. This can usually be added to the SOLR_OPTS environment variable in your solr.in.sh script file. E.g.:

- Stop Solr
- Windows: Edit your **solr.in.cmd** file to include:
  set SOLR_OPTS=%SOLR_OPTS% -Ddisable.configEdit=true
- Start Solr

The following command can be used to validate, if it is in fact disabled:

```
curl http://localhost:8983/solr/tts-server/config -H "Accept: application/json" -H "Content-type:application/json" -d "{'set-user-property' : {'variable_name':'some_value'}}"
```

*Please note: Adjust the **URL** and the **core name** where appropriate. A 403 status code will be returned if it has been successfully disabled.*