Product Support Notice

PSN #	PSN005960u

Original publication date: 15-Dec-21. This is issue #06, published date: 3-Feb-22.

Severity/risk level	High	Urgency	Immediately

Name of problem Avaya Analytics for Oceana Log4j vulnerabilities

Products affected

Avaya Analytics for Oceana 4.1.0.0, 4.1.0.1, 4.1.1.0

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security* - ***Apache Log4j Vulnerability - Impact for Avaya products*** on support.avaya.com for updates.

Avaya Analytics for Oceana 4.1.0.0, 4.1.0.1, 4.1.1.0 are impacted by the Log4j vulnerabilities CVE-2021-44228, CVE-2021-45046.
Avaya Analytics for Oceana 4.1.0.0, 4.1.0.1, 4.1.1.0 are not impacted by CVE-2021-45105, CVE-2021-44832, CVE-2021-4104.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.
Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

Avaya Analytics 4.1.1 Patch 8 and Avaya Analytics 4.1.0.1 Patch 8 are available to download from support.avaya.com.
Installing this patch will resolve Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046) for both Avaya Analytics 4.1.1 and Avaya Analytics 4.1.0.1 releases.
This is a mandatory patch that Avaya recommends that all existing Analytics customers must apply for Avaya Analytics 4.1.1.0 and Avaya Analytics 4.1.x releases.

- Note that the workaround below is no longer the recommended for the Avaya Analytics 4.1.1 and Avaya Analytics 4.1.x releases and is superseded by the relevant patch.

Workaround or alternative remediation

The following mitigation steps provide limited protection and are no longer recommended. Avaya recommends customers update to Avaya Analytics 4.1.1 Patch 8 or Avaya Analytics 4.1.0.1 Patch 8

This procedure should only be executed by a solution engineer who is familiar with Analytics
Note that when the procedure is carried out per steps below the MSTR-SVR pod will not need to be restarted and thus the workaround to license expiry (ref. PSN005928u) will not need to be applied again as a result of this procedure.

Apply service level mitigation Configuration for Historical Reporting:
It is recommended to enable the java parameter "formatMsgNoLookups=true". After applying the parameter, the java service must be restarted for the new parameter to take effect.

1. Log onto CCM and switch to root user.
2. List all mstr pods

```
[root@env1-ccm cust]# k get po -n mstr
NAME                  READY   STATUS    RESTARTS   AGE
mstr-md-689797f885-nnhkf    1/1     Running   1          7d
mstr-srv-6bfd644984-hhgn9   1/1     Running   0          4d1h
mstr-web-84f97b87c5-xb74d   1/1     Running   0          4d6h
```

3. Exec onto the mstr-srv pod (note the pod name will be different on your system).

```
[root@env1-ccm cust]# k exec -it mstr-srv-6bfd644984-hhgn9 -n mstr bash
bash-4.2#
```

4. Find MSIReg.reg file and make a backup of the file.

```
bash-4.2# find / -name MSIReg.reg
/var/opt/microstrategy/MSIReg.reg
bash-4.2# cp /var/opt/microstrategy/MSIReg.reg /var/opt/microstrategy/MSIReg.reg.backup
bash-4.2#
```

5. Open the file for editing

```
bash-4.2# vi /var/opt/microstrategy/MSIReg.reg
```

6. You will need to locate all keys ending in “JVM Options”
   Such as:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\MicroStrategy\JNI Bridge\Config for DataServices\JVM Options]
```

7. Modify the parameter “Other Options” to have the value ‘-Dlog4j2.formatMsgNoLookups=true’. It should look like:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\MicroStrategy\JNI Bridge\Config for DataServices\JVM Options]
"OtherOptions"="-Dlog4j2.formatMsgNoLookups=true"
```

8. Confirm that the updated file looks like below:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\MicroStrategy\JNI Bridge\Config for DataServices\JVM Options]
"OtherOptions"="-Drefine.verbosity=error;-Dlog4j2.formatMsgNoLookups=true"
[HKEY_LOCAL_MACHINE\SOFTWARE\MicroStrategy\JNI Bridge\Configuration\JVM Options]
"OtherOptions"="-Dlog4j2.formatMsgNoLookups=true"
"HeapMaxSize"="256M"
```

9. Locate the start.sh file and create a backup of it.

```
bash-4.2# find / -name start.sh
/var/opt/microstrategy/install/ModelingService/bin/start.sh
bash-4.2# cp /var/opt/microstrategy/install/ModelingService/bin/start.sh
/var/opt/microstrategy/install/ModelingService/bin/start.sh.original
bash-4.2#
```

10. Edit /var/opt/microstrategy/install/ModelingService/bin/start.sh file

```
bash-4.2# vi /var/opt/microstrategy/install/ModelingService/bin/start.sh
```

11. Search for "$java_cmd" in the file and add -Dlog4j2.formatMsgNoLookups=true after the "$java_cmd". For example, change from:

```
"$java_cmd" $MODELSERVICE_JAVA_GARBAGE_COLLECTION
$MODELSERVICE_JAVA_USER_TZ $MODELSERVICE_JAVA_INITIAL_MEMORY
$MODELSERVICE_JAVA_MAX_MEMORY $MODELSERVICE_PLAY_CONF_FILE
$MODELSERVICE_JAVA_KERB_CONF
$MODELSERVICE_JAVA_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR
$MODELSERVICE_JAVA_HEAP_DUMP_PATH -cp "./lib/com.microstrategy.modelservice-launcher.jar" play.core.server.ProdServerStart
```

to:

```
"$java_cmd" -Dlog4j2.formatMsgNoLookups=true
$MODELSERVICE_JAVA_GARBAGE_COLLECTION $MODELSERVICE_JAVA_USER_TZ
$MODELSERVICE_JAVA_INITIAL_MEMORY $MODELSERVICE_JAVA_MAX_MEMORY
$MODELSERVICE_PLAY_CONF_FILE $MODELSERVICE_JAVA_KERB_CONF
$MODELSERVICE_JAVA_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR
```

$MODELSERVICE_JAVA_HEAP_DUMP_PATH -cp "./lib/com.microstrategy.modelservice-launcher.jar" play.core.server.ProdServerStart

12. Restart the Intelligence Server

/var/opt/microstrategy/bin/mstrctl -s IntelligenceServer stop

13. Wait for the Intelligent Server to automatically start up. You can confirm the Intelligence Server is running again by checking the ‘state’ field in the below command output.

```
bash-4.2# /var/opt/microstrategy/bin/mstrctl -s IntelligenceServer gs
<status>
    <computer_name>mstr-srv-6bfd644984-hhgn9</computer_name>
    <login>mstr</login>
    <process_id>568</process_id>
    <process_creation_time>2021-12-10 10:29:52.640Z</process_creation_time>
    <boot_time>2021-12-06 11:19:01.000Z</boot_time>
    <state can_be_paused="0">running</state>
    <execution_mode>service</execution_mode>
    <version_info>
        <file_version>11.2.0400.40296</file_version>
        <file_description>11.2.0400.40296</file_description>
        <company_name>MicroStrategy Incorporated</company_name>
        <original_filename>libMSTRSvr2.so~</original_filename>
        <product_name>MicroStrategy 2020</product_name>
        <product_version>11.2.4</product_version>
        <legal_copyright>Copyright (c) 2000-2021 MicroStrategy Incorporated. All rights reserved.</legal_copyright>
        <legal_trademarks>MicroStrategy (r) is a registered trademark of MicroStrategy Incorporated</legal_trademarks>
        <build_machine_name>ip-10-244-21-14.internal.microstrategy.com</build_machine_name>
    </version_info>
    <application>
        <version>11.2.0400.40296</version>
        <tcp_port_number>34952</tcp_port_number>
        <rest_port_number>34962</rest_port_number>
    </application>
    <memory>
        <logging_time>2021-12-10 10:29:57.305</logging_time>
        <memory_state>normal</memory_state>
    </memory>
</status>
```

14. Locate pdfexporter.sh and run the stop command

```
bash-4.2# find / -name pdfexporter.sh
/var/opt/microstrategy/install/Export/pdfexporter.sh
bash-4.2# /var/opt/microstrategy/install/Export/pdfexporter.sh stop
Attempt to stop PDF Export Service...
bash-4.2#
```

15. Edit /var/opt/microstrategy/install/Export/pdfexporter.sh and Add “-Dlog4j2.formatMsgNoLookups=true” after nohup "JAVA_BIN" as below

```
 nohup "$JAVA_BIN" -Dlog4j2.formatMsgNoLookups=true -Djava.library.path="${DLE_INSTALL_LOCATION}" -Xms512m -Xmx${heap_size}m -cp "${SCRIPT_PATH}/PDFExporterService.jar":"${DLE_INSTALL_LOCATION}/com.datalogics.PDFL.jar" org.springframework.boot.loader.JarLauncher --spring.config.location="${SCRIPT_PATH}/application.properties" > /dev/null 2>&1 < /dev/null & echo $! > "${PID_FILE}"
```

16. Start the Export Engine

```
bash-4.2# /var/opt/microstrategy/install/Export/pdfexporter.sh start
```

Attempt to start PDF Export Service...
PDF Export Service is started.

17. Run the following commands to check all your changes are still there after the Export Engine has started.

```
bash-4.2# cat /var/opt/microstrategy/MSIReg.reg  | grep formatMsgNoLookups
"OtherOptions"="-Drefine.verbosity=error;-Dlog4j2.formatMsgNoLookups=true"
"OtherOptions"="-Dlog4j2.formatMsgNoLookups=true"
bash-4.2# cat /var/opt/microstrategy/install/Export/pdfexporter.sh  | grep formatMsgNoLookups
    nohup "$JAVA_BIN" -Dlog4j2.formatMsgNoLookups=true -
Djava.library.path="${DLE_INSTALL_LOCATION}" -Xms512m -Xmx${heap_size}m -cp
"${SCRIPT_PATH}/PDFExporterService.jar":"${DLE_INSTALL_LOCATION}/com.datalogics.PDFL.ja
r" org.springframework.boot.loader.JarLauncher --
spring.config.location="${SCRIPT_PATH}/application.properties" > /dev/null 2>&1 < /dev/null & echo $!
> "${PID_FILE}"
```

18. Exit out of the mstr-srv pod back to CCM

Remarks
Issue 1 – December 15, 2021: Initial publication. Issue 2 – December 17, 2021: Updates to refer to CVE-2021-45046 and other clarifications. There were NO changes to the mitigation procedure provided under “Apply service level mitigation Configuration for Historical Reporting” Issue 3 – December 21, 2021: Updates to refer to CVE-2021-45105 and other clarifications. There were NO changes to the mitigation procedure provided under “Apply service level mitigation Configuration for Historical Reporting” Issue 4 – January 06, 2022: Updates to refer to CVE-2021-44832 and CVE-2021-4104. There were NO changes to the mitigation procedure provided under “Apply service level mitigation Configuration for Historical Reporting” Issue 5 – January 27, 2022: Updates to Resolution Section to reference 4.1.1. Patch 8. There were NO changes to the mitigation procedure provided under “Apply service level mitigation Configuration for Historical Reporting” Issue 6 – February 3, 2022: Updates to Resolution Section to reference 4.1.0.1. Patch 8. There were NO changes to the mitigation procedure provided under “Apply service level mitigation Configuration for Historical Reporting”

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch	
Always	
Download	
n/a.	
Patch install instructions	**Service-interrupting?**
n/a	Yes
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
n/a	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046 Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105 Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832 Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104

Reference https://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

As noted in this PSN.

If you require further information or assistance, please contact your Authorized Service Provider or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.