Security Advisory Report - OBSO-2201-01

Apache Log4j JMSAppender Class Configuration Property Handling JNDI Lookup Local Privilege Escalation Weakness (CVE-2021-4104)

Release Date:	2022-01-18 16:47:01
Last Update:	2022-05-06 09:38:33
Version:	1.15

Summary

JMSAppender in Log4j 1.2 is vulnerable to JNDI injection when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228.

The rating for this vulnerability is medium to high.

Details

Apache Log4j contains a flaw that is triggered as the JMSAppender class can trigger a JNDI lookup via the 'TopicBindingName' or 'TopicConnectionFactoryBindingName' configuration properties. An attacker can use that JNDI lookup to gain remote code execution in a similar fashion to CVE-2021-44228.

The vulnerability may be exploited if the following requirements are met:

1. The application must use log4j and the JMSAppender for logging, for example either in *log4j.properties*, or in *log4j.xml*:

- log4j.appender.X=org.apache.log4j.net.JMSAppenderlog4j.appender.X=org.apache.log4j.net.JMSAppender
- <appender name="console" class="org.apache.log4j.net.JMSAppender">

An application doesn't have to utilize JMSAppender to be affected, since an attacker with local write access could edit the configuration file and add the JMSAppender themselves.

2. The values of the TopicBindingName, or the TopicConnectionFactoryBindingName properties should be set using untrusted input. This may either be done programmatically, using *setTopicConnectionFactoryBindingName* (or *setTopicBindingName*), or it can be done via a configuration change with the appropriate local write access privileges.

3. Since log4j 1.x doesn't auto-reload its configuration when changed, an attacker might have to force

log4j to reload it to make it active (e.g. via application restart).

Products are not affected:

- If log4j is not installed on the system.

- Or if log4j is installed but not being used by the application for logging.

- Or if the JMSApenderClass is not installed on the system

- Or after log4J V1 has been updated to either reload4J (latest) or log4J V2

Products are affected (high severity):

- If log4j is used by the application for logging.

- If the JMSAppender is used and the values of *TopicBindingName* or *TopicConnectionFactoryBindingName* are being set using untrusted user input, by a remote attacker.

CVSSv3 Score: 7.5 (AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

- If the JMSAppender isn't being used, but the JMSAppender.class is included in the log4j-1.2.x.jar. and If log4j configuration files (.properties, .xml) are writable by low privileged users.

Products are affected (medium severity):

- If log4j is used by the application for logging.

- and if the JMSAppender isn't being used, but the JMSAppender.class is included in the log4j-1.2.x.jar.

- and if log4j configuration files (.properties, .xml) are writable only by high-privileged users.

CVSSv3 Score: 6.4 (AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

Affected Products

Products that are confirmed not affected

Circuit
Circuit Meeting Room V1
Atos Unify OpenScape Voice (duplex deployments) V9 an V10
Atos Unify OpenScape Cordless IP V2
Atos Unify OpenScape First Response ESRP V9
Atos Unify OpenScape First Response BCF V10
Atos Unify OpenScape First Response ESAAP V1
Atos Unify OpenScape First Response PSS V1
Atos Unify OpenScape First Response MSBF V2
Atos Unify OpenScape Alarm Response Professional V4 and V5
Atos Unify Virtual Care Collaboration Service V1
Atos Unify OpenScape Xpert Clients V6 and V7
Atos Unify OpenScape Xpert MLC V6 and V7
Atos Unify OpenScape Branch V9 and V10
Atos Unify OpenScape SBC V9 and V10
Atos Unify OpenScape Contact Media Service V11 R0.0.2 and higher
OpenScape Contact Center Extensions V3
Atos Unify OpenScape UC Application V9 and V10
Atos Unify OpenScape Web Collaboration V7
Atos Unify OpenScape Concierge V4
Atos Unify OpenScape Media Server V9
Atos Unify OpenScape Common Management Platform V7 and V10
Atos Unify OpenScape Composer V2
Atos Unify OpenScape Accounting Management V3, V4 and V5
Atos Unify OpenScape Voice Trace Manager V8
Atos Unify OpenScape Voice Survival Authority
Atos Unify OpenScape Desk Phones CP SIP
Atos Unify OpenScape Desk Phones CP HFA
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
OpenStage HFA V3
OpenStage SIP V3
Atos Unify OpenScape WLAN Phone WL3 and WL4
Atos Unify OpenScape DECT Phone S5 and S6
Atos Unify OpenScape DECT Phone SL5 and SL6
Atos Unify OpenScape WLAN Phone Wireless Service Gateway
AC Win SL V3
HiPath DS-Win V4 version 4.6.29.0 and higher???????
Atos Unify OpenScape Backup & Recovery Services

Atos Unify OpenScape Sesap V2
Atos Unify OpenScape License Management CLA/CLM
Atos Unify OpenScape Fault Management V10R0.07.31, V11R0.01.28, V12R0.00.09 and higher
Atos Unify Professional Services – Solutions Framework V4 / V5 (PSSF V4/V5)
Atos Unify OpenScape Personal Edition V7
Atos Unify OpenScape Fusion for Office V1 and V2
Atos Unify OpenScape Extensions for MS Outlook V1 and V2
Atos Unify OpenScape 4000 Platform V8 R2.22.10/V10 R0.28.7 and higher
Atos Unify OpenScape 4000 Assistant V8 R2.22.16/V10 R0.28.10 and higher
Atos Unify OpenScape 4000 CSTA V8 R2.22.12/V10 R0.28.8 and higher
Atos Unify OpenScape 4000 Loadware V8 V8R2.22.18 and higher V10 R0.28.11 and higher
Atos Unify OpenScape 4000 Manager V8 R2.22.16 /V10 R0.28.10 and higher
Atos Unify OpenScape Deployment Service V7.0 R3.88.5 / V10 R2.3.0 and higher
Atos Unify OpenScape Contact Center V11R0.2.0 and higher
HiPath CAP V3.0.R16.034.2 and higher

Products that are confirmed affected (high severity)

Atos Unify OpenScape 4000 V8 and V10 Softgate Loadware only (LW-Hotfix before V8R2.22.18 and LW-Hotfix before V10 R0.28.11) (available)
See additional notes for the OpenScape 4000 Softgate Loadware
HiPath CAP V3.0 before Hotfix V3.0.R16.034.1 is available, JMSAppender class is removed)
HiPath CAP V3.0 (Hotfix V3.0.R16.034.2 is available, updated to reload4j)

Products that are confirmed affected (medium severity)

Atos Unify OpenScape 4000 Platform V8 before V8 R2.22.10 (available)
Atos Unify OpenScape 4000 V8 Assistant before VV8 R2.22.16 (available)
Atos Unify OpenScape 4000 V8 CSTA before V8 R2.22.12 (available)
Atos Unify OpenScape 4000 Manager V8 before V8 R2.22.16 (available)
Atos Unify OpenScape 4000 Platform V10 before V10 R0.28.7 (available)
Atos Unify OpenScape 4000 V10 Assistant before V10 R0.28.10(available)
Atos Unify OpenScape 4000 V10 CSTA before V10 R0.28.8 (available)
Atos Unify OpenScape 4000 Manager V10 before V10 R0.28.10 (available)
Atos Unify OpenScape Xpert System Manager V6 and V7 (Update to log4J V2.17.1 is planned in V7 R4 for 30.4.2022)
Atos Unify OpenScape Contact Center V10 and V11 before V11R0.2.0 (update to Log4j V2.17.1 is planned in V10R4.3.0 for 6.5.2022)
Atos Unify OpenScape Contact Media Service V10 and V11 (update to reload4j planned in V11 R0.2.0 planned for May 13th)
Atos Unify OpenScape Deployment Service V7 before V7.0 R3.88.5 and V10 before V10 R2.3.0 (available)
Atos Unify OpenScape Fault Management V10 before V10R0.07.31 , V11 before V11R0.01.28 and V12 before V12R0.00.09 (available)
Atos Unify OpenScape First GEMMA V2 and V3 (Update to Log4J V2 is planned for V3)
Atos Unify OpenScape Enterprise Express V9 and V10 (see section notes and check affected products)
Atos Unify OpenScape Voice (simplex deployments) V9 an V10 (see section notes and check affected products)
Atos Unify OpenScape Xpressions V7 (XPR V7 R1 FR5 HF40 (ApplicationBuilder-811FR5-19085) and

earlier, fixes available in V7 R1 FR5 HF40 P908 (available) and V7 R1 FR5 HF40 P911 (available), see notes for Xpressions)
Atos Unify OpenScape OpenScape Fusion for Notes V1 and V2 (update to reload4j is planned for V1R8.32.0 and V2R1.15.0 (available))
Atos Unify OpenScape Business V3 (update to log4jV2 is planned for Q2/2022, see notes)
HiPath DS-Win V4 version older than 4.6.29.0 (update to HiPath DS-Win version V4 R6.32.0 or higher recommended)

Updates for products that are evaluated not affected and are using log4jV1

Atos Unify OpenScape UC Application V9 and V10 (Update to reload4j is planned for V10 R3: 27.5.2022 / V9R4: 10.6.2022)
Atos Unify OpenScape Media Server V9 (Update to reload4j is released with the updates for UC V10 and V9R4)
OpenScape Voice Survival Authority (Update to reload4j is pending / new plan date is published when available)
Atos Unify OpenScape Composer V2 (Update to reload4j is pending / new plan date is published when available)

Notes for Atos Unify OpenScape Business:

OpenScape Business does not utilize JMSAppender (CVE-2021-4104), JMSSink (CVE-2022-23302), JDBCAppender CVE-2022-23305), Chainsaw CVE-2022-23307) and SMTPAppender (CVE-2020-9488) . Therefore OpenScape Business is not affected by default. As a prerequisite to expose the OpenScape Business an attacker needs root access, has to edit the log4j configuration file and add the JMSAppender themselves.

The risk for OpenScape Business X V3 is low as SSH port 22 is disabled by factory default. The OpenScape Business individual dynamic root login credentials are not available in general as they are machine generated on demand.

To minimize the risk for the OpenScape Business S / UC Booster Server it is recommend that the SSH interface port stays disabled within the firewall settings, as the SSH is not used by OpenScape Business S / UC Booster Server (check via Yast). If SSH interface is enabled (not recommended) on the Linux server make sure to use a strong root password and follow the instruction of the Security Checklist.

OpenScape Business Clients are not affected.

The update to log4jV2 is planned for OpenScape Business V3R2.

Notes for Atos Unify OpenScape Enterprise Express V9 and V10 the evaluation of the following products apply:
If a product is affected, please follow the advisory for the respective product
Atos Unify OpenScape Voice (duplex deployments) V9 an V10
Atos Unify OpenScape Common Management Platform V7 and V10
Atos Unify OpenScape Deployment Service V7 and V10
Atos Unify OpenScape UC Application V9 and V10
Atos Unify OpenScape Media Server V9

Atos Unify OpenScape Concierge V4
Atos Unify OpenScape Contact Center V10
Atos Unify OpenScape Xpressions V7
Atos Unify OpenScape Voice Trace Manager V8

Notes for Atos Unify OpenScape Voice (simplex deployments) V9 an V10
Atos Unify OpenScape Voice (duplex deployments) V9 an V10
Atos Unify OpenScape Common Management Platform V7 and V10
Atos Unify OpenScape Deployment Service V7 and V10
Atos Unify OpenScape UC Application V9 and V10
Atos Unify OpenScape Media Server V9

Notes for the OpenScape 4000 Softgate Loadware:

The SoftGate Loadware is used in the following Software Deployments:
• SoftGate StandAlone
• Survivable SoftGate
• Integrated SoftGate on Simplex
• Integrated SoftGate on Enterprise Gateway
• Integrated SoftGate on Duplex
• Enterprise Gateway
• Survivable Enterprise Gateway
• STMIX

Additional fix information:

OpenScape Xpressions V7:
ApplicationBuilder-811FR5-20907
HOTFIX OPENSCAPE XPRESSIONS V7 R1 FR5 HF40 P908
Removed JDBCAppender, JMSAppender, JMSSink, SocketServer. and SMTP Appender. Additionally whole chainsaw package was removed from log4j V1 package

HOTFIX OPENSCAPE XPRESSIONS V7 R1 FR5 HF40 P911
ApplicationBuilder-811FR5-20911
HF006202
Update of log4jV1 to reload4j

Recommended Actions

Update to fixed versions when available.

References

External References

- https://www.suse.com/security/cve/CVE-2021-4104.html
- https://nvd.nist.gov/vuln/detail/CVE-2021-4104
- https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126
- http://slf4j.org/log4shell.html
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://security.snyk.io/vuln/SNYK-JAVA-LOG4J-2316893
- https://reload4j.qos.ch/

Version Change History

Version	Date	Description
1.0	18.01.2022	- Initial release
1.1	19.01.2022	- If the JMSApenderClass is not installed on the system (not affected) - HiPath CAP Hotfix V3.0 R16.34.1 released - OS4K Loadware Hotfix V10R0.28.10 / V8R2.22.17 planned for 21.01.2022 - CMS V11 R0.0.2 - Log4j 2.17.1, Log4j1 is available - Atos Unify OpenScape First Response PSS V1 (not affected) - Atos Unify OpenScape First Response MSBF V2 (not affected) - Atos Unify OpenScape First GEMMA V2 and V3 (affected / medium) - Atos Unify OpenScape Backup & Recovery Services (not affected) - Atos Unify OpenScape Common Management Platform V7 and V10 (not affected) - Atos Unify OpenScape Composer V2 (not affected) - Atos Unify OpenScape Enterprise Express V9 and V10 (affected / medium) - Atos Unify OpenScape Voice (simplex deployments) V9 an V10 (affected / medium)
1.2	20.01.2022	- Notes for the Softgate Loadware added - Atos Unify Professional Services – Solutions Framework V4 / V5 (PSSF V4/V5) (not affected)
1.3	27.01.2022	- OpenScape 4000 Loadware (LW-Hotfix V8R2.22.17 and Specific LW-Hotfix V10 R0.28.10 is available - Fix plan for OpenScape 4000 V8R2 and V10 added - Atos Unify OpenScape Xpressions V7 (XPR V7 R1 FR5 HF40 (ApplicationBuilder-811FR5-19085) and earlier, fix planned) - Gemma V3: Update to log4J V2 is planned
1.4	02.02.2022	- Products are not affected after log4J V1 has been updated to either reload4J (latest) or log4J V2 - OpenScape Personal Edition V7 (not affected) - OpenScape Fusion for Notes V1 and V2 (affected/medium) - Atos Unify OpenScape Business V3 (affected/medium)

1.5	04.02.2022	- Explicitly listed UC Clients OpenScape Fusion for Office V1 and V2 and OpenScape Extensions for MS Outlook V1 and V2 (Not affected) - DLS V10 update to reload4j planned for for 11.2.2022
1.6	09.02.2022	- Notes for OpenScape Business within the Affected Products section - OpenScape Xpressions fix is available in: ApplicationBuilder-811FR5-20907 HOTFIX OPENSCAPE XPRESSIONS V7 R1 FR5 HF40 P908
1.7	14.02.2022	- JMSSink (CVE-2022-23302), JDBCAppender CVE-2022-23305), Chainsaw CVE-2022-23307) and SMTPAppender (CVE-2020-9488) not used in OpenScape Business - Atos Unify OpenScape Deployment Service V7 and V10 (update to reload4j planned for V10 for 25.2.2022)
1.8	22.02.2022	- OpenScape Fusion for Notes V2R1.15.0 includes Reload4j 1.2.18.4 is available - OpenScape Business V3 (update to log4jV2 is planned for Q2/2022) - OpenScape 4000 V8 and V10 product family (for V8 update to reload4j planned for 01.04.2022 / For V10 update to reload4j planned for 18.3.2022) - OpenScape Xpert System Manager V7 (Update to log4J V2.17.1 is planned in V7 R4 for 30.4.2022) - OpenScape Contact Center V10,V11 (Update to log4J V2.17.1 is planned in V11R0.2.0 for 25.3.2022, update to reload4j is planned in V10R4.2.0 for 25.3.2022) - OpenScape Contact Media Service V10 and V11 (update to reload4j planned in V11 R0.2.0 planned for April 1st) - OpenScape Fault Management V10 (Update for reload4j is planned in V10R0.07.31 for 04.03.2022) - Updates for products that are evaluated not affected and are using log4jV1 - OpenScape UC Application V9 and V10 (Update to reload4j is planned until 30.4.2022) - OpenScape Media Server V9 (Update to reload4j is planned until 30.4.2022) - OpenScape Voice Survival Authority (Update to reload4j is planned until 30.4.2022) - OpenScape Composer V2 (Update to reload4j is planned until 30.4.2022)
1.9	07.03.2022	- Xpression Update to reload4j i XPRESSIONS V7 R1 FR5 HF40 P911 (available) - HiPath DS-Win V4 version older than 4.6.29.0 (update to HiPath DS-Win version V4 R6.32.0 or higher recommended)
1.10	09.03.2022	- OS4K and the Manager V10 R0 are now free of the vulnerable log4j V1 framework it has been replaced by reload4J (details see Affected Products section) - Update OpenScape 4000 V8 and V10 Softgate Loadware to LW-Hotfix V8R2.22.18 and LW-Hotfix V10 R0.28.11
1.11	15.03.2022	- log4jV1 updated to reaload4j in OpenScape Deployment Service V10 R2.3.0 - OS Fault Management V10R0.07.31 is updated to log4j 2.17.1
1.12	23.03.2022	- OpenScape Deployment Service updated to reload4j in V7.0 R3.88.5
1.13	28.03.2022	- OpenScape Contact Center V11R0.2.0 updated to log4J V2.17.1 - OpenScape Contact Center V10 (update to Log4j V2.17.1 is planned in V10R4.3.0 for 6.5.2022)
1.14	11.04.2022	- Upates for OpenScape 4000 V8 are available
1.15	06.05.2022	- Plan dates for UC and Media Server (V10 R3: 27.5.2022 / V9R4: 10.6.2022) - Plan dates for OpenScape Composer, Survival Authority are pending - Contact Media Service V11R0.2.0 is planned for 13.05.2022 - HiPath CAP Hotfix V3.0.R16.034.2 is available, updated to reload4j

Advisory: OBSO-2201-01, status: general release
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com