Support Note DirX-15:

DirX Products and Apache Log4j Vulnerability CVE-2021-44228

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

CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

Severity: Critical

Base CVSS Score: 10.0 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Versions Affected: all log4j-core versions >=2.0-beta9 and <=2.14.1

Descripton: Apache Log4j <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default.

DirX Directory (all supported versions)

Analysis: DirX Directory does not use Log4j, therefore it **is not affected** by this vulnerability.

Mitigation: No action necessary.

DirX Identity (all supported versions)

Analysis: DirX Identity uses Log4j

V1.2.8 in

- the Java Server
- WebCenter
- REST Services.

V1.2.17 in

- Active MQ Message Broker.

Log4j 1.2x **is not affected** by this vulnerability.

Mitigation: No immediate action necessary.

Note: As Log4j V1.2 reached End-of-Life since August 2015 the next release of DirX Identity will contain the latest released version where the issue is fixed.

DirX Audit (all supported versions)

Analysis: DirX Audit uses Log4j V1.2.17. This version **is not affected** by this vulnerability.

Mitigation: No immediate action necessary.

Note: As Log4j V1.2 reached End-of-Life since August 2015 the next release of DirX Audit will contain the latest released version where the issue is fixed.

DirX Access (all supported versions)

Analysis: DirX Access uses Log4j V2.8. This version **is affected** by this vulnerability.

Mitigation: The affected versions of Log4j libraries can be upgraded to the newest versions without any impact on functioning of the system. This solution has been successfully tested and is described in section **Manual Upgrade**. This approach is applicable on any patch version of DirX Access, hence, is simple comparing to application of newest (cumulative) patch that might bring additional changes requiring longer testing in target environment first.

Latest by end of Tuesday 14th December 2021 there will be patches for DirX Access V8.9, V8.10 and V9.0 that replaces the vulnerable component with log4j V2.15 which closes the vulnerability.

Any custom extension modules (callouts) used in the environment need to be examined for the use of the vulnerable Log4j versions. The official extension modules (e.g., DXA Audit Plugin) will be patched in week 13th – 17th December 2021 according to their priority.

Manual Upgrade:

Depending on the version and configuration, the changes need to be applied on following subset of components DXA Services container, DXA WebApplications container, PEPs, Policy Manager. After the change, each component has to be restarted.

DXA Services container

- Upload following jars into {*installation folder*}/Services/plugins

```
log4j-api-2.15.0.jar

log4j-core-2.15.0.jar

log4j-jul-2.15.0.jar

log4j-slf4j-impl-2.15.0.jar
```

- Replace following lines in {*installation folder*}/Services/instances/{*instance name*}/configuration/org.eclipse.equinox.simpleconfigurator/bundles.info

```
org.apache.logging.log4j.api,2.8.0,../../plugins/log4j-api-2.8.jar,2,true

org.apache.logging.log4j.core,2.8.0,../../plugins/log4j-core-2.8.jar,2,true

org.apache.logging.log4j.jcl,2.8.0,../../plugins/log4j-jcl-2.8.jar,2,false

org.apache.logging.log4j.jul,2.8.0,../../plugins/log4j-jul-2.8.jar,2,false
org.apache.logging.log4j.slf4j-impl,2.8.0,../../plugins/log4j-slf4j-impl-2.8.jar,2,false
```

by lines

```
org.apache.logging.log4j.api,2.15.0,../../plugins/log4j-api-2.15.0.jar,2,true

org.apache.logging.log4j.core,2.15.0,../../plugins/log4j-core-2.15.0.jar,2,true

org.apache.logging.log4j.jul,2.15.0,../../plugins/log4j-jul-2.15.0.jar,2,false

org.apache.logging.log4j.slf4j-impl,2.15.0,../../plugins/log4j-slf4j-impl-2.15.0.jar,2,false
```

- Replace following lines in {*installation folder*}/Services/instances/{*instance name*}/etc/wrapper.conf

```
wrapper.java.classpath.4=../../plugins/log4j-core-2.8.jar

wrapper.java.classpath.5=../../plugins/log4j-api-2.8.jar

wrapper.java.classpath.6=../../plugins/log4j-jul-2.8.jar
```

by lines

```
wrapper.java.classpath.4=../../plugins/log4j-core-2.15.0.jar

wrapper.java.classpath.5=../../plugins/log4j-api-2.15.0.jar

wrapper.java.classpath.6=../../plugins/log4j-jul-2.15.0.jar
```

DXA WebApplications container

- Upload following jars into {*installation folder*}/WebApplications/plugins

```
log4j-api-2.15.0.jar

log4j-core-2.15.0.jar

log4j-jul-2.15.0.jar

log4j-slf4j-impl-2.15.0.jar
```

The artifacts shall be taken from Log4j project official repository.

- Replace following lines in {*installation folder*}/WebApplications/instances/{*instance name*}/configuration/org.eclipse.equinox.simpleconfigurator/bundles.info

```
org.apache.logging.log4j.api,2.8.0,../../plugins/log4j-api-2.8.jar,2,true

org.apache.logging.log4j.core,2.8.0,../../plugins/log4j-core-2.8.jar,2,true

org.apache.logging.log4j.jcl,2.8.0,../../plugins/log4j-jcl-2.8.jar,2,false

org.apache.logging.log4j.jul,2.8.0,../../plugins/log4j-jul-2.8.jar,2,false

org.apache.logging.log4j.slf4j-impl,2.8.0,../../plugins/log4j-slf4j-impl-2.8.jar,2,false
```

by lines

```
org.apache.logging.log4j.api,2.15.0,../../plugins/log4j-api-2.15.0.jar,2,true

org.apache.logging.log4j.core,2.15.0,../../plugins/log4j-core-2.15.0.jar,2,true

org.apache.logging.log4j.jul,2.15.0,../../plugins/log4j-jul-2.15.0.jar,2,false

org.apache.logging.log4j.slf4j-impl,2.15.0,../../plugins/log4j-slf4j-impl-2.15.0.jar,2,false
```

- Replace following lines in {*installation folder*}/WebApplications/instances/{*instance name*}/etc/wrapper.conf

```
wrapper.java.classpath.4=../../plugins/log4j-core-2.8.jar

wrapper.java.classpath.5=../../plugins/log4j-api-2.8.jar

wrapper.java.classpath.6=../../plugins/log4j-jul-2.8.jar
```

by lines

```
wrapper.java.classpath.4=../../plugins/log4j-core-2.15.0.jar

wrapper.java.classpath.5=../../plugins/log4j-api-2.15.0.jar

wrapper.java.classpath.6=../../plugins/log4j-jul-2.15.0.jar
```

Policy Manager

- Upload following jars into {*installation folder*}/PolicyManager/plugins

```
log4j-api-2.15.0.jar

log4j-core-2.15.0.jar
```

```
log4j-jul-2.15.0.jar

log4j-slf4j-impl-2.15.0.jar
```

The artifacts shall be taken from Log4j project official repository.

- Replace following lines in {*installation folder*}/PolicyManager/instances/{*instance name*}/configuration/org.eclipse.equinox.simpleconfigurator/bundles.info

```
org.apache.logging.log4j.api,2.8.0,../../plugins/log4j-api-2.8.jar,2,true

org.apache.logging.log4j.core,2.8.0,../../plugins/log4j-core-2.8.jar,2,true

org.apache.logging.log4j.jcl,2.8.0,../../plugins/log4j-jcl-2.8.jar,2,false

org.apache.logging.log4j.jul,2.8.0,../../plugins/log4j-jul-2.8.jar,2,false

org.apache.logging.log4j.slf4j-impl,2.8.0,../../plugins/log4j-slf4j-impl-2.8.jar,2,false
```

by lines

```
org.apache.logging.log4j.api,2.15.0,../../plugins/log4j-api-2.15.0.jar,2,true

org.apache.logging.log4j.core,2.15.0,../../plugins/log4j-core-2.15.0.jar,2,true

org.apache.logging.log4j.jul,2.15.0,../../plugins/log4j-jul-2.15.0.jar,2,false

org.apache.logging.log4j.slf4j-impl,2.15.0,../../plugins/log4j-slf4j-impl-2.15.0.jar,2,false
```

PEPs

- Replace vulnerable versions of Log4j libraries by newest versions in folder with libraries of respective PEP container. No configuration changes necessary.