Security Advisory (OBSO2112-01) - Supplementary Information for Atos Unify OpenScape UC V9 and V10 (Atos internal, Registered Customers and Partners)

KB000102540

☆ ☆ ☆ ☆ ☆ 12 views

This information is subject to change

Document type	Vulnerability Impact Statement
Author	OpenScape Baseline Security Office
Document Status	Released
Document Classification	Atos internal, Registered Customers and Partners
Affected Products	Atos Unify OpenScape UC V9R4 and V10
Affected CPEs and criticality	CVE-2021-44228 (https://nvd.nist.gov/vuln/detail/CVE-2021-44228) (Critical) CVE-2021-45046 (https://nvd.nist.gov/vuln/detail/CVE-2021-45046) (Low)
Affected component	log4j2.x
Affected component versions	CVE-2021-44228: log4j2.x before version 2.15 CVE-2021-45046: log4j2.x before version 2.16

Open Scape V9 R4

Impact	**OpenScape V9 R4 is not affected**
Impact Description	The latest released version OpenScape UC 9.4.59.0 uses version log4j 1.2 in various components. The critical vulnerability only affects log4j 2.x before version 2.15. OpenScape UC V9.4.59.0 is thus not affected by the vulnerability CVE-2021-44228. The subsequently identified vulnerability CVE-2021-45046 (criticality=low) also affects log4j 2.x. The OpenScape UC component SyncUC is using the library log4j 2.3, however the exploit for CVE-2021-44228 is not applicable as there is no client interface available with input fields providing this operation. The vulnerability CVE-2021-4104 (criticality=medium) identified in the disclosure affects version log4j 1.x. The vulnerability can only be exploited if the JMSAppender functionality is used. For OpenScape UC this functionality is not used. OpenScape UC is therefore not affected by CVE-2021-4104.
Available Workarounds	Not applicable

Fix version	Not planned

Open Scape UC V10

Impact	**OpenScape UC V10.2.9.0 and higher are affected**
Impact Description	The OpenScape V10 uses version log4j 1.2 and in various components. The critical vulnerability only affects log4j 2.x before version 2.15. Log4j 2 is used in OpenFire 4.5.4 which has been introduced in OpenScape UC V10.2.9.0 and is used in versions thereafter. The subsequently identified vulnerability CVE-2021-45046 (criticality=low) also affects log4j 2.x. Hence both CVEs are affecting OpenScape UC V10.2.9.0 and higher. The OpenScape UC component SyncUC is using the library log4j 2.3, however the exploit for CVE-2021-44228 is not applicable as there is no client interface available with input fields providing this operation. The vulnerability CVE-2021-4104 (criticality=medium) identified in the disclosure affects version log4j 1.x. The vulnerability can only be exploited if the JMSAppender functionality is used. For OpenScape UC this functionality is not used. OpenScape UC is therefore not affected by CVE-2021-4104.
Available Workarounds	The instructions to apply this workaround in the openfire (both the embedded and the external openfire) are the following: • Stop openfire with **/etc/init.d/openfire stop** • Edit the startup script **/etc/init.d/openfire** (be sure to keep the same owner and file permissions as before) changing the point where **OPENFIRE_OPTS** variable is defined by adding the JVM argument: **-Dlog4j2.formatMsgNoLookups=true** So the result after the change should be: OPENFIRE_OPTS="${OPENFIRE_OPTS} -DopenfireHome=${OPENFIRE_HOME} -DopenfireLogDir=${OPENFIRE_LOGDIR} -Dopenfire.lib.dir=${OPENFIRE_LIB} -Dlog4j.configurationFile=${OPENFIRE_HOME}/conf/log4j.xml **-Dlog4j2.formatMsgNoLookups=true**" Start again openfire with **/etc/init.d/openfire start**
Fix version	The workaround is planned for V10R3 FR10 HF1

Last modified 1 hour ago
Products:
Customers:

☆ ☆ ☆ ☆ ☆ 12 views

***** - This article solved my issue without the need to open a ticket

**** - This article helped me close a ticket

*** - It helped me with the issue, but didn't provide a complete solution

** - This article didn't help me much/is missing attachments or links

* - This article is outdated/is missing information/contains an error/has a wrong explanation

Leave a comment