Chapril - Demande #5707

Le SI du Chapril est-il vulnérable à la faille Log4shell ? Si oui, il faut mettre en place les mesures correctives

13/12/2021 13:37 - Frédéric Couchet

Statut:	Fermé	**Début:**	13/12/2021
Priorité:	Immédiate	**Echéance:**	
Assigné à:	Romain H.	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Sprint 2022 décembre		

Description

Sur https://logging.apache.org/log4j/2.x/index.html "The Log4j team has been made aware of a security vulnerability, CVE-2021-44228, that has been addressed in Log4j 2.15.0."

La faille est appelée Log4Shell.

Le SI du Chapril est-il vulnérable à la faille Log4shell ? Si oui, il faut mettre en place les mesures correctives.

Le ticket côté April https://agir.april.org/issues/5706

Demandes liées:

Lié à visio.chapril.org - Demande #5705: Vérifier la correction de log4shell	**Fermé**	**11/12/2021**

Historique

#3 - 13/12/2021 13:47 - Frédéric Couchet

- Description mis à jour

#4 - 13/12/2021 13:47 - Frédéric Couchet

il y a un fil sur le forum chatons https://forum.chatons.org/t/log4j-java-et-cve-2021-44228-log4shell/3069

#5 - 13/12/2021 15:14 - Frédéric Couchet

- Lié à Demande #5705: Vérifier la correction de log4shell ajouté

#6 - 15/12/2021 16:39 - Pierre-Louis Bonicoli

- Pour la machine grof, les paquets liblog4j1.2-java et liblog4j2-java ne sont pas installés. Les paquets openjdk-11-jre-headless et ca-certificates-java sont présents. Étant donné qu'à ma connaissance ils ne sont pas utilisés et parce que liblog4j pourrait être *bundlé* , je propose de les supprimer.

#7 - 15/12/2021 16:48 - Pierre-Louis Bonicoli

Une discussion au sujet de la faille sur le forum chatons.

#8 - 16/12/2021 09:58 - Quentin Gibeaux

je lance le même find qu'à l'april sur l'infra

#9 - 16/12/2021 13:48 - Frédéric Couchet

Le bulletin d'alerte du CERT-FR (régulièrement mis à jour) https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

#10 - 16/12/2021 13:48 - Frédéric Couchet

Pierre-Louis Bonicoli a écrit :

> - Pour la machine grof, les paquets liblog4j1.2-java et liblog4j2-java ne sont pas installés. Les paquets openjdk-11-jre-headless et ca-certificates-java sont présents. Étant donné qu'à ma connaissance ils ne sont pas utilisés et parce que liblog4j pourrait être *bundlé* , je propose de les supprimer.

C'est toi qui connaît le mieux la VM. Si tu penses qu'il faut supprimer les paquets fais-le stp.

#11 - 16/12/2021 15:18 - Quentin Gibeaux

```
===== bastion =====
Connection to bastion.cluster.chapril.org closed.
===== admin =====
Connection to admin.cluster.chapril.org closed.
===== dns =====
Connection to dns.cluster.chapril.org closed.
===== mail =====
Connection to mail.cluster.chapril.org closed.
===== pouet =====
Connection to pouet.cluster.chapril.org closed.
===== sympa =====
Connection to sympa.cluster.chapril.org closed.
===== lamp =====
/srv/chaprilinfos/log4j.properties
Connection to lamp.cluster.chapril.org closed.
===== pad =====
/var/www/etherpad-lite-1.8.6/src/node_modules/log4js/test/log4js.json
/var/www/etherpad-lite-1.8.6/src/node_modules/log4js/lib/log4js.js
/var/www/etherpad-lite-1.8.6/src/node_modules/log4js/lib/log4js.json
/var/www/etherpad-lite-1.8.4/src/node_modules/log4js/test/log4js.json
/var/www/etherpad-lite-1.8.4/src/node_modules/log4js/lib/log4js.js
/var/www/etherpad-lite-1.8.4/src/node_modules/log4js/lib/log4js.json
/var/www/etherpad-lite-1.8.7/src/node_modules/log4js/test/log4js.json
/var/www/etherpad-lite-1.8.7/src/node_modules/log4js/lib/log4js.js
/var/www/etherpad-lite-1.8.7/src/node_modules/log4js/lib/log4js.json
/var/www/etherpad-1.8.4-test/src/node_modules/log4js/test/log4js.json
/var/www/etherpad-1.8.4-test/src/node_modules/log4js/lib/log4js.js
/var/www/etherpad-1.8.4-test/src/node_modules/log4js/lib/log4js.json
Connection to pad.cluster.chapril.org closed.
===== libreoffice =====
channel 0: open failed: connect failed: No route to host
stdio forwarding failed
ssh_exchange_identification: Connection closed by remote host
===== valise =====
find: ‘/proc/169840/task/169840/net’: Argument invalide
find: ‘/proc/169840/net’: Argument invalide
find: ‘/proc/170310/task/170310/net’: Argument invalide
find: ‘/proc/170310/net’: Argument invalide
find: ‘/proc/172206/task/172206/net’: Argument invalide
find: ‘/proc/172206/net’: Argument invalide

Connection to valise.cluster.chapril.org closed.
===== xmpp =====
Connection to xmpp.cluster.chapril.org closed.
===== drop =====
Connection to drop.cluster.chapril.org closed.
===== allo =====
/usr/share/jitsi-videobridge/lib/log4j-api-2.15.0.jar
/usr/share/jitsi-videobridge/lib/log4j-core-2.15.0.jar
/etc/jitsi/videobridge/log4j2.xml
Connection to allo.cluster.chapril.org closed.
===== ludo =====
Connection to ludo.cluster.chapril.org closed.
===== biliz =====
Connection to biliz.cluster.chapril.org closed.
===== catom =====
channel 0: open failed: connect failed: No route to host
stdio forwarding failed
ssh_exchange_identification: Connection closed by remote host
===== grof =====
Connection to grof.cluster.chapril.org closed.
===== maine.chapril.org =====
Connection to maine.chapril.org closed.
===== coon.chapril.org =====
Connection to coon.chapril.org closed.
===== felicette.orbite.chapril.org =====
Connection to felicette.orbite.chapril.org closed.
```

Il y a donc des choses à voir sur lamp, allo

#12 - 16/12/2021 21:52 - Romain H.

Pour lamp j'ai désactivé la tâche cron qui lance ce code il y a quelques jours par mesure de précaution.

Il faudrait voir comment mettre à jour la bibliothèque avant de la réactiver.

#13 - 03/01/2022 18:04 - François Poulain

Faudrait épouiller les jar qui tournent s'il y en a.

#14 - 04/02/2022 14:45 - Frédéric Couchet

- Assigné à mis à Romain H.

pour statoolinfos et log4j voir https://forum.chatons.org/t/log4j-java-et-cve-2021-44228-log4shell/3069/18

#15 - 07/04/2022 10:31 - Pierre-Louis Bonicoli

- Version cible changé de Sprint 2021 décembre à Sprint 2022 avril

#16 - 12/05/2022 09:26 - Pierre-Louis Bonicoli

- Version cible changé de Sprint 2022 avril à Backlog

#17 - 03/12/2022 08:06 - Pierre-Louis Bonicoli

- Statut changé de Nouveau à Résolu

- Version cible changé de Backlog à Sprint 2022 décembre

- % réalisé changé de 0 à 100

statoolinfos ne tourne plus (#5985).

#18 - 06/12/2022 22:22 - Quentin Gibeaux

- Statut changé de Résolu à Fermé