# Rapport d'analyse Vitam/Vitam-UI sur la faille log4j et procédure de correction

> Note that only the log4j-core JAR file is impacted by this vulnerability. Applications using only the log4j-api JAR file without the log4j-core JAR file are not impacted by this vulnerability.

## Versions utilisées et impacts

- R13
    - ELK 7.6.0 => Conseil upgrade en 7.16.1
        - Logstash utilise log4j-core-2.12.1.jar
        - Kibana: Non impacté.
    - Vitam
        - log4j: 2.13.0 => Conseil upgrade en 2.15.0
        - logbook: log4j-core-2.13.0
    - Mongo 4.2.2-1: Non impacté.
- R16
    - ELK 7.8.1 => Conseil upgrade en 7.16.1
        - Logstash utilise log4j-core-2.12.1.jar
        - Kibana: Non impacté.
    - Vitam
        - log4j: 2.13.0 => Conseil upgrade en 2.15.0
        - logbook: log4j-core-2.13.0
    - VitamUI: Non impacté.
    - Mongo 4.2.5-1: Non impacté.
    - Grafana/Prometheus: Non impacté.
- v5RC
    - ELK 7.13.4 => Conseil upgrade en 7.16.1
        - Logstash utilise log4j-core-2.14.0.jar
        - Kibana: Non impacté.
    - Vitam
        - log4j: 2.13.0 => Conseil upgrade en 2.15.0
        - logbook utilise log4j-core-2.13.0.jar
    - VitamUI: Non impacté.
    - Mongo 4.2.5-1: Non impacté.
    - Grafana/Prometheus: Non impacté.

En résumé, seul les composants `vitam-logbook, Elasticsearch (data & log) & logstash` sont impactés par cette faille de sécurité.

> En alternative à la montée de version des composants, qui sera mise en oeuvre dans des versions bugfixes de Vitam, une procédure peut être mise en oeuvre à court terme pour sécuriser le produit.

> Celle-ci consiste notamment en la modification de fichiers de configuration et de paramétrage Java des modules concernés. La mise en oeuvre de cette procédure est décrite ci-dessous.

## Sources officielles

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
- https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb
- https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
- https://logging.apache.org/log4j/2.x/security.html

---

## Procédure Patch log4j Vitam

> INFO: Dans la suite de cette procédure, remplacez <INVENTORY_FILE> par le fichier d'inventaire adéquat.

### Mise à jour des sources de déploiement

Installer la commande `patch` sur la machine à partir de laquelle vous allez exécuter le déploiement pour appliquer le patch fourni.

Récupérer le fichier diff en fonction de la version de vos sources de déploiement et le mettre à la racine du répertoire deployment/.

Appliquer le patch pour les sources de déploiement à partir de la racine de `deployment/`:

- Pour la R16/v5RC: `patch -p1 < 8674.diff`
- Pour la R13: `patch -p1 < 8690-r13.diff`
- Pour la R9: `patch -p1 < 8689-r9.diff`

  > Attention: En R9, le nom des groupes de l'inventaire est constitué avec de `-` et non de `_`. Il faudra éditer dans la suite de cette procédure les groupes associés pour prendre en considération cette particularité. ex. modifiez `hosts_logbook` en `hosts-logbook`.

### Vérification avant de débuter

> INFO: À effectuer uniquement à partir du site primaire.

- S'assurer qu'il n'y a plus de workflow en cours ni en FATAL

```
ansible-playbook ansible-vitam-exploitation/check_workflow_status.yml
--vault-password-file vault_pass.txt -i environments/<INVENTORY_FILE>
```

Exemple de résultat:

```
TASK [check_workflow_fatal : get the total of workflow KO]
*********************
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=2)
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=3)
ok: [vitam-access-external] => (item=3)
ok: [vitam-access-external] => (item=1)
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=0)
ok: [vitam-access-external] => (item=0)
```

Cette liste ne doit être constité que de `item=0`, si ce n'est pas le cas, se connecter sur les tenants correspondants pour appliquer les procédures adéquates.

- Éteindre les externals et les timers pour s'assurer qu'aucune action ne sera exécuté durant la procédure.

```
ansible-playbook ansible-vitam-exploitation/stop_external.yml --vault-
password-file vault_pass.txt -v -i environments/<INVENTORY_FILE>
ansible-playbook ansible-vitam-exploitation/stop_vitam_timers.yml --
vault-password-file vault_pass.txt -v -i environments/<INVENTORY_FILE>
```

> INFO: En cas d'installation multi-site, il est recommandé d'appliquer la procédure suivante sur le site secondaire avant d'appliquer sur le site primaire.

## Suppression des classes JndiLookup dans la librairie log4j-core

**Installation de la commande zip sur les vms hébergeant la librairie log4j-core**

- Pour CentOS

```
ansible
hosts_logbook,hosts_logstash,hosts_elasticsearch_log,hosts_elasticsearch_da
ta -a 'yum install -y zip' --vault-password-file vault_pass.txt -i
environments/<INVENTORY_FILE>
```

- Pour Debian

```
ansible
hosts_logbook,hosts_logstash,hosts_elasticsearch_log,hosts_elasticsearch_da
ta -a 'apt install -y zip' --vault-password-file vault_pass.txt -i
environments/<INVENTORY_FILE>
```

**Suppression de la classe JndiLookup pour chacun des composants impactés**

```
ansible hosts_logbook -a "bash -c 'zip -q -d /vitam/lib/logbook/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class'" --vault-password-file vault_pass.txt -i environments/<INVENTORY_FILE>

ansible hosts_logstash -a "bash -c 'zip -q -d /usr/share/logstash/logstash-core/lib/jars/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class'" --vault-password-file vault_pass.txt -i environments/<INVENTORY_FILE>

ansible hosts_elasticsearch_log,hosts_elasticsearch_data -a "bash -c 'zip -q -d /usr/share/elasticsearch/lib/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class'" --vault-password-file vault_pass.txt -i environments/<INVENTORY_FILE>
```

> Si `FAILED | rc=127 >> bash: zip : command not foundnon-zero return code` La commande zip n'est pas installée sur les vms.
>
> Si `FAILED | rc=12 >> zip error: Nothing to do! (/vitam/lib/logbook/log4j-core-2.13.0.jar)non-zero return code` La classe a déjà été retirée, vous pouvez ignorer ce message.
>
> Sinon le retour est `CHANGED | rc=0`.

## Mise à jour de la configuration ElasticSearch (data & log) & Logstash

> INFO: En R9, il faut éditer ce playbook pour modifier le nom des groupes pour changer les `_` en `-`.

Copier le fichier `playbook_elk_log4j.yml` sous ansible-vitam/ puis exécutez la commande suivante:

```
ansible-playbook ansible-vitam/playbook_elk_log4j.yml --vault-password-file vault_pass.txt -v -i environments/<INVENTORY_FILE>
```

Exemple de output:

```
TASK [logstash : apply configuration files] ***********************************
changed: [vitam-logstash] => (item=jvm.options)
ok: [vitam-logstash] => (item=log4j2.properties)
ok: [vitam-logstash] => (item=startup.options)
ok: [vitam-logstash] => (item=logstash.yml)

RUNNING HANDLER [restart logstash] ********************************************
changed: [vitam-logstash]
```

```
TASK [elasticsearch-cluster : apply logging for elasticsearch configuration
file]
ok: [vitam-elasticsearch] => (item=log4j2.properties)
changed: [vitam-elasticsearch] => (item=jvm.options)

RUNNING HANDLER [elasticsearch-cluster : restart service]
**********************
changed: [vitam-elasticsearch]
```

## Mise à jour des composants Vitam

Mettre à jour les composants Vitam à l'aide du tag update_jvmoptions_vitam

```
ansible-playbook ansible-vitam/vitam.yml --vault-password-file
vault_pass.txt -v --tags update_jvmoptions_vitam -i
environments/<INVENTORY_FILE>
```

Exemple de changed ansible pour chacun des services Vitam:

```
TASK [vitam : Deploy common configuration files in sysconfig subdir]
***********
changed: [vitam-host] => (item=java_opts)

RUNNING HANDLER [vitam : restart the service]
*********************************
changed: [vitam-host]
```

## Redémarrage des timers

> INFO: Les externals ont été redémarrés lors de l'exécution de la commande précédente.

```
ansible-playbook ansible-vitam-exploitation/start_vitam_timers.yml --vault-
password-file vault_pass.txt -v -i environments/<INVENTORY_FILE>
```

---