Guide d’analyse des vulnérabilités et rappel des mesures d’hygiène

FR_Centreon_Guide_Analyse_vulnérabilités_V1_2021_02_17

centreon

Sommaire

Introduction 3

1 Contrôler votre version 5

2 Contrôler l'existence de fichiers « illégitimes » 6

2.1 Contrôle des fichiers 6

2.2 Analyse Yara 6

2.2.1 Si vous avez installé Centreon par les sources : 7

2.2.2 Si vous avez installé Centreon par les RPMs : 7

3 Analyser votre réseau 8

3.1 Snort/Suricata - Détection du Webshell P.A.S. 8

3.2 Snort/Suricata - Détection Exaramel 8

4 Renforcer la sécurité / Durcir votre OS 9

5 Garder vos plateformes à jour et sécurisées 10

6 Cloisonner votre réseau 11

7 Surveiller votre plateforme 12

8 Sauvegarder et exporter les journaux d'événements 13

9 Pour aller plus loin 14

Introduction

L'ANSSI a publié, le 15 février 2021, un rapport [1] sur une faille de sécurité supposée de la plateforme logicielle de supervision Centreon. Ce rapport pourrait conduire à penser que les solutions commercialisées par Centreon présenteraient des failles de sécurité. Ce communiqué précise la position de Centreon à l'aune des connaissances actuelles concernant la campagne identifiée et de ses échanges avec l'ANSSI. Centreon appelle, par ailleurs, les entreprises et organisations publiques au respect des règles d'hygiène informatique et à utiliser de préférence les versions mises à jour et supportées de ses solutions.

[1] https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-004/

Centreon a communiqué le 16 février 2020 sur la campagne d'attaques dont certains utilisateurs ont été la cible. Centreon tient à apporter des précisions importantes quant à cet évènement. Nous vous invitons à prendre connaissance des informations afin de mieux comprendre ce qu'il s'est réellement passé.

Pour rappel :

- **MANQUE D'HYGIÈNE INFORMATIQUE**

  L'attaque décrite par l'ANSSI concerne exclusivement des versions obsolètes du logiciel open source de Centreon. En effet, l'ANSSI précise que la version la plus récente concernée par cette campagne est la version 2.5.2, sortie en Novembre 2014. Cette version n'est non seulement plus supportée depuis plus de 5 ans, mais a semble-t-il également été déployée sans respect de sécurisation des serveurs et des réseaux, notamment des connexions vers l'extérieur des entités concernées. Depuis cette version, Centreon a publié 8 versions majeures. Centreon rappelle l'importance du respect des bonnes pratiques de l'hygiène informatique et des recommandations d'installation et de sécurisation des logiciels de l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

- **PAS DE CLIENTS IMPACTÉS**

  Selon les échanges des dernières 24 heures avec l'ANSSI, aucun client de Centreon n'a été impacté. L'ANSSI précise que seule une quinzaine d'entités ont été la cible de cette campagne, et qu'elles sont toutes utilisatrices d'une version open source obsolète (v2.5.2), qui n'est plus supportée depuis 5 ans. Centreon contacte actuellement tous ses clients et partenaires afin de les accompagner vers une vérification de leurs installations et l'application des bonnes pratiques d'hygiène informatique.

- **PAS DE PROPAGATION DE CODE MALICIEUX**

  Le rapport de l'ANSSI et nos échanges avec ces derniers confirment que Centreon n'a pas distribué ou contribué à propager de code malicieux. Il ne s'agit pas d'une attaque de type supply chain et aucun parallèle avec d'autres attaques de ce type ne peut être fait dans ce cas.

- **CAMPAGNE TERMINÉE**

  Par ailleurs, l'ANSSI précise que la campagne en question est terminée et qu'aucune activité malicieuse n'est à observer à l'heure actuelle.

- **RECOMMANDATION**

  Centreon recommande à tous les utilisateurs ayant encore une version obsolète de son logiciel open source de le mettre à jour ou de contacter Centreon et son réseau de partenaires certifiés.

Cette campagne concerne exclusivement des versions obsolètes du logiciel open source de Centreon (datant de Novembre 2014).

Pour plus d'informations veuillez consulter notre communiqué de presse « Centreon apporte des éclaircissements suite à la parution du rapport de l'ANSSI ».

Centreon vous accompagne en 9 points, afin d'identifier la compromission identifiée par l'ANSSI et vous guider dans la sécurisation de votre plateforme.

1. Contrôler votre version
2. Contrôler l'existence de fichiers "illégitimes"
3. Vérifier la compromission de votre installation
4. Durcir votre OS
5. Garder vos plateformes à jour et sécurisées
6. Cloisonner votre réseau
7. Surveiller votre plateforme
8. Sauvegarder et exporter les journaux d'événements
9. Pour aller plus loin

1 Contrôler votre version

Centreon a mis en place une politique claire de gestion de la vie des versions de ses produits. Il est important pour tout utilisateur de suivre ces recommandations et garder ses plateformes à jour en fonction des releases pour se protéger et éviter tout problème de sécurité.

A date, Centreon supporte les versions suivantes de son produit (hors contrat spécifique) :

- 20.10
- 20.04
- 19.10

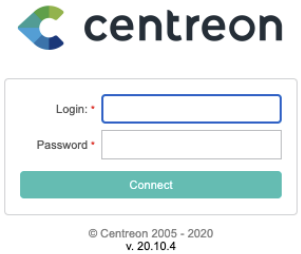
Toutes les autres versions ne sont plus maintenues ni supportées par Centreon. Si vous avez des versions plus anciennes, nous vous appelons à faire le nécessaire pour les mettre à jour soit par vos soins soit via un partenaire certifié par Centreon.

Plusieurs méthodes sont proposées pour vérifier votre version :

- Via la page de login [1a]
- Via l'interface Web et le menu "Administration" - "About" (ou À propos)
- Via une commande en cli : `rpm -qa | grep centreon-web`

Vous trouverez également dans les liens ci-dessous notre politique sur le cycle de vie de notre logiciel [1b], notre Release Notes [1c] ainsi qu'un flux RSS vous permettant de faire de la veille [1d].

[1a]



[1b] https://docs.centreon.com/current/fr/releases/lifecycle.html
[1c] https://docs.centreon.com/current/fr/releases/introduction.html
[1d] https://github.com/centreon/centreon/releases.atom

2 Contrôler l'existence de fichiers « illégitimes »

2.1 Contrôle des fichiers

Les fichiers suivants ne sont pas développés par Centreon :

- `/usr/local/centreon/www/search.php`
- `/usr/share/centreon/www/search.php`
- `/usr/share/centreon/www/modules/Discovery/include/DB-Drop.php`
- `/usr/share/centreon/www/centreon_module_linux_app64`
- `/usr/local/centreon/www/modules/centreon_module_linux_app64`

Portez une attention particulière aux chemins des répertoires indiqués.

Le fichier suivant – `/usr/share/centreon/www/htmlHeader.php` - existait sur les versions 2.5 de Centreon et vous ne devriez pas l'avoir sur une version récente. Si vous disposez de ce fichier à cet emplacement, contactez-nous.

Ce fichier a été déplacé à l'emplacement
`/usr/share/centreon/www/include/core/header/htmlHeader.php`

Ce fichier est légitime et a passé différents contrôles avec succès (Code Pull Request Review, analyse statique SonarQube) qui n'ont pas relevé de vulnérabilité. Nous restons cependant vigilants et continuons nos investigations.

2.2 Analyse Yara

L'ANSSI met à disposition différents moyens permettant la détection de la compromission.
Vérifier les prérequis suivants :

- unzip
- curl
- Dépôt EPEL (pour CentOS 7)

L'installation de l'outil Yara et ses règles associées sont décrites plus bas.

Pour plus d'informations au sujet de Yara rendez-vous sur le site officiel
https://yara.readthedocs.io/en/stable/gettingstarted.html

A date de la rédaction du document, les commandes suivantes sont à exécuter (sous CentOS 7)

```
# Installation de Yara
yum install yara --enablerepo=epel

# Téléchargement du fichier de règles
curl -LJO http://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-IOC-002-YARA.zip
unzip CERTFR-2021-IOC-002-YARA.zip -d CERTFR-2021-IOC-002-YARA
cd CERTFR-2021-IOC-002-YARA
```

2.2.1 Si vous avez installé Centreon par les sources :

Le chemin par défaut est `/usr/local/src/`
Note : Changez le chemin en fonction de votre installation

```
# Exécution de Yara dans le dossier CERTFR-2021-IOC-002-YARA/
yara --recursive exaramel.yara /tmp
yara --recursive exaramel.yara /etc/init/
yara --recursive exaramel.yara /etc/init.d/
yara --recursive exaramel.yara /etc/systemd/system/

yara --recursive fobushell_perl_scripts.yara /usr/local/src/
yara --recursive fobushell_sqldump.yara /usr/local/src/
yara --recursive fobushell.yara  /usr/local/src/
yara --recursive fobushell_zip_archive.yara  /usr/local/src/
```

2.2.2 Si vous avez installé Centreon par les RPMs :

Le chemin par défaut est `/usr/share/centreon/` :

```
# Exécution de Yara dans le dossier CERTFR-2021-IOC-002-YARA/
yara --recursive exaramel.yara /tmp
yara --recursive exaramel.yara /etc/init/
yara --recursive exaramel.yara /etc/init.d/
yara --recursive exaramel.yara /etc/systemd/system/

yara --recursive fobushell_perl_scripts.yara /usr/share/centreon/
yara --recursive fobushell_sqldump.yara /usr/share/centreon/
yara --recursive fobushell.yara /usr/share/centreon/
yara --recursive fobushell_zip_archive.yara /usr/share/centreon/
```

Si la commande ne vous retourne rien, cela veut dire que votre installation n'est pas compromise.

Si vous avez un doute, l'équipe de support (support@centreon.com ou https://support.centreon.com) reste à votre disposition pour répondre à vos interrogations.

3 Analyser votre réseau

Si ces règles (Webshell et Exaramel) vous remontent des alertes, suivez vos procédures de sécurité habituelles (Plan de Réponse à Incident).

3.1 Snort/Suricata - Détection du Webshell P.A.S

Les règles de détection SNORT sont disponibles depuis le site du CERT https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-002/.

Afin d'installer ces règles, nous vous invitons à consulter la documentation officielle de Snort https://www.snort.org/documents/snort-users-manual-html

3.2 Snort/Suricata - Détection Exaramel

D'après les analyses de l'ANSSI (page 38 du rapport FR) la communication avec le serveur de contrôle de Exaramel est protégée par l'implémentation TLS. Il est de ce fait délicat de procéder à une détection réseau en utilisant les outils snort/suricata.

4 Renforcer la sécurité / Durcir votre OS

Centreon supporte par défaut la distribution Linux CentOS 7. Il est impératif d'appliquer les meilleures pratiques de sécurité.

Nous vous invitons à suivre les recommandations de l'ANSSI « *Recommandations de sécurité relatives à un système gnu/linux* ».

Important : Les guides sont des documents techniques qu'il est souhaitable de suivre cependant, tout n'est pas forcément applicable et un mauvais paramétrage peut entraîner l'indisponibilité de votre plateforme (ex. : SELinux n'est compatible qu'à partir de la version 20.10 de Centreon).

5 Garder vos plateformes à jour et sécurisées

Un autre aspect essentiel est la sécurité de votre plateforme Centreon. Différents points sont à prendre en compte et vous pouvez vous fier à notre documentation pour :

- Ajouter le chiffrement (https ou tls) [5a]
  - Sur vos flux exposés (interface d'administration de Centreon)
  - Sur vos flux non exposés (flux entre serveurs Centreon)
- Renforcer la sécurité des comptes
  - Portez une attention particulière sur la création des comptes
    - Suivez le principe du moindre privilège, notamment sur les comptes de services et/ou de checks
    - Protégez les comptes d'accès à vos bases de données (Map, MBI, central, etc.)
- Mettre à jour votre plateforme
- Utilisez de préférence SNMPv3
- Utilisez le chiffrement avec NRPE

[5a] https://docs.centreon.com/current/fr/administration/secure-platform.html (Centreon open source), https://docs.centreon.com/current/fr/graph-views/secure-your-map-platform.html (pour server MAP) et la mise à jour vers la 20.10, dernière version à jour, https://docs.centreon.com/current/fr/update/update-centreon-platform.html

6 Cloisonner votre réseau

Assurez-vous d'avoir renforcé la sécurité de vos serveurs avant de les exposer sur Internet. Le serveur Centreon ne devrait jamais être exposé en frontal à Internet et devrait être protégé/cloisonné par des mécanismes intermédiaires, à minima un reverse proxy et un WAF (Web Application Firewall) pour l'accès Web.

Les flux doivent impérativement être chiffrés et l'utilisation de certificat client TLS est fortement recommandé.

Nous vous invitons à suivre les « *Recommandations relatives à l'interconnexion d'un Système d'Information à Internet* » proposés par l'ANSSI.

Vous devez également autoriser les flux sortants afin de bénéficier des services suivants :

- CEIP (Customer Experience Improvement Program)
- active licences
- Enterprise Plugin Packs
- AI/ML services (beta)
- Proactive Support (beta)
- Yum repositories (for install/update RPM packages)

Les adresses à autoriser sur votre proxy sortant sont :

- https://statistics.centreon.com
- https://api.imp.centreon.com
- https://api.a.prod.mycentreon.com
- https://yum.centreon.com/standard/

Noter que l'ensemble des URLs est en HTTPS.

7 Surveiller votre plateforme

Que ce soit la partie matérielle ou la partie logicielle, surveiller l'intégrité de votre plateforme. Différents outils sont à votre disposition dont Ossec, Wazuh ou pour une utilisation plus autonome, Tripwire et Aide.

https://www.ossec.net
https://wazuh.com
https://www.tripwire.com
https://aide.github.io

Ces outils vous permettront notamment de contrôler l'intégrité des fichiers en surveillant les répertoires critiques. Tout ajout ou modification fera l'objet d'une alerte que vous pourrez traiter.

8 Sauvegarder et exporter les journaux d'événements

Les meilleures pratiques recommandent d'exporter les journaux et de les conserver 3 mois « live » et 1 an au repos.

9 Pour aller plus loin

Nous pensons que le code open source est plus sûr par nature que le code propriétaire.

Comme pour tous les logiciels open source, vous avez accès à notre code hébergé sur les dépôts publics GitHub (https://github.com/centreon). Vous pouvez analyser, contribuer, améliorer et suivre les modifications du code.

Ce code doit être protégé par votre infrastructure. Nous vous recommandons fortement de suivre les meilleures pratiques en termes de sécurité, en suivant le guide de « Recommandations pour la protection des Systèmes d'Information essentiels » mis à disposition par l'ANSSI.

