Vulnerability Analysis Guide and Reminder of Healthy Measures

c centreon

Summary

Introduction

ANSSI published a report on February 15, 2021 presenting a suspected security vulnerability in the Centreon monitoring software platform. This report could mislead individuals to believe that the solutions provided by Centreon would present security flaws.

In accordance with exchanges between Centreon and ANSSI, this press release clarifies the facts in light of the best knowledge available regarding the identified campaign. In addition, Centreon calls on companies and public organizations to respect the ANSSI IT Health Recommendations and to preferably use updated and supported versions of its solutions, especially within the context of production environments.

Centreon published on February 16, 2021 a Press Release in order to provide important clarification:

- **IMPORTANCE OF FOLLOWING IT SECURITY RECOMMENDATIONS**

  The campaign described by ANSSI exclusively concerns obsolete versions of Centreon's open source software. Indeed, the ANSSI specifies that the most recent version concerned by this campaign is version 2.5.2, released in November 2014. This version is not only no longer supported (and has not been for more than 5 years), but has also apparently been deployed without sufficient respect for the security of servers and networks, including connections outside the entities concerned. Since this version, Centreon has released 8 major versions. Centreon reminds its users of the importance of complying with ANSSI IT Health guidelines and recommendations for installing and securing software.

- **NO CUSTOMERS IMPACTED**

  It is confirmed by ANSSI that Centreon customers were not impacted. According to discussions over the past 24 hours with ANSSI, only about fifteen entities were the targets of this campaign, and they are all users of an obsolete open source version (v2.5.2), which has been unsupported for 5 years. Centreon is currently contacting all of its customers and partners to assist them in verifying their installations are up-to-date and in compliance with ANSSI's guidelines for a Healthy Information System.

- **NO PROPAGATION OF MALICIOUS CODE**

  The ANSSI report and direct exchanges with it confirm that Centreon did not distribute or contribute to propagate malicious code. This is not a supply chain type attack and no parallel with other attacks of this type can be made in this case.

- **CAMPAIGN COMPLETED**

  In addition, ANSSI specifies that the campaign in question is over and that no malicious activity can be observed at this time.

- **RECOMMENDATION**

  Centreon recommends that all users who still have an obsolete version of its open source software in production update it to the latest version or contact Centreon and its network of certified partners.

Centreon supports you in 9 points, in order to identify the compromise identified by ANSSI and guide you in securing your platform.

1. Check your current version
2. Check the existence of "illegitimate" files
3. Analyze your network
4. Enhance Security / Harden your Centreon installation OS
5. Keep your Centreon platforms up to date and secure
6. Partition your network
7. Monitor the platform integrity
8. Backup and export event logs
9. Going further

1   Check your current version

Centreon set up a clear policy for managing its product life cycle. It is important that all users follow these recommendations and keep their platforms up to date to protect themselves and avoid any security issues.

To date, Centreon supports the following versions of its product (excluding specific contract):
- 20.10
- 20.04
- 19.10

All the other versions are no longer maintained or supported by Centreon. If you have old versions, we invite you to take the necessary measures to update them either by yourself or via a partner certified by Centreon.

Several methods are available to check your version:
- Via the login page [1a]
- Via the Centreon Web interface: "Administration" - "About"
- Via the command line on your Centreon server: `rpm -qa | grep centreon-web`

You will also find in the links below our policy on the software lifecycle [1b], our Release Notes [1c] as well as an RSS feed allowing you to remain informed [1d].

[1a]

centreon

Login: * [_____]
Password * [_____]

Connect

© Centreon 2005 - 2020
v. 20.10.4

[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   Check the existence of "illegitimate" files

2.1   Files checks

These following files identified in the ANSSI report are not provided by 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`

Please pay particular attention to the paths of the directories.

The following file – `/usr/share/centreon/www/htmlHeader.php` - existed on the older version of Centreon (2.7 and before) and you must not have it on the most recent versions. If you have this file on this path, please contact us.

This file was moved to
`/usr/share/centreon/www/include/core/header/htmlHeader.php`

This file is legitimate and has successfully passed various checks (Code Pull Request Review, SonarQube static analysis) which did not reveal any vulnerabilities. However, we remain vigilant and continue our investigations.
.

2.2   Yara analysis

ANSSI provides various tools to detect the compromise.

Prerequisite:
- unzip
- curl
- EPEL repository (for CentOS 7)

Please find below the instructions for installing Yara, the tool used by ANSSI and its rules.

For further information, please consult the official documentation of Yara:
https://yara.readthedocs.io/en/stable/gettingstarted.html

Please follow the instructions below (tested under CentOS 7 at the time of writing)

```
# Install Yara from EPEL repository
yum install yara --enablerepo=epel

# Download & unzip the Yara rules from CERT
mkdir CERTFR-2021-IOC-002-YARA
cd CERTFR-2021-IOC-002-YARA
curl -LJO http://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-IOC-002-
YARA.zip
unzip CERTFR-2021-IOC-002-YARA.zip
```

2.2.1   If you installed Centreon from the source

The default installation path is `/usr/local/src/`
Note: Change the Centreon path according to your installation

```
# Execute 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   If you installed Centreon from the RPM

The default installation path is `/usr/share/centreon/`

```
# Execute 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/
```

If the command returns nothing, it means that your installation is not compromised.

If you have any doubt about the result, please contact our Support team: support@centreon.com
- https://support.centreon.com).

3   Analyze your network

If you got some alerts from these rules (Webshell or Exaramel), you have to follow your usual safety procedures (incident response plan).

3.1   Snort/Suricata - Webshell P.A.S detection

You can download the Snort rules from the CERT https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-002/.

For further information about Snort, please consult the Snort official documentation: https://www.snort.org/documents/snort-users-manual-html

3.2   Snort/Suricata – Exaramel detection

According to the ANSSI report (page 36 in the EN version), Exaramel uses HTTPS to communicate with its Command and Control server. No unusual parameters are used, which does not enable the identification of Exaramel communications.

It is therefore difficult to perform a network detection using the snort / suricata tools.

4   Enhance Security / Harden your Centreon installation OS

Centreon supports the Linux Centos 7 distribution by default. It is imperative to apply the security recommendations proposed by ANSSI.

We recommend that you follow the ANSSI guide "Configuration Recommendations of a GNU/Linux System".

Important: guides are technical documents that you are advised to follow, however, not everything is necessarily applicable and please note that incorrect settings may cause your platform to be unavailable. (for example, SELinux compatibility has only been available since Centreon 20.10's release)

5 Keep you Centreon platforms up to date and secure

Another essential aspect is the security of your Centreon platforms. There are different points to consider and you can rely on our documentation to:

- Enable encryption (https or tls) [5a]
    - On your exposed flows (Centreon Web interface)
    - On your internal or unexposed flows (flows between servers or Centreon components)
- Strengthen account security
    - Pay particular attention to the account usage
        - Follow the principle of least privilege, especially on service and / or check accounts
        - Protect access accounts to your databases (Map, MBI, central, etc.)
- Update your platform;
- Preferably use SNMPv3
- Use encryption with NRPE

[5a] https://docs.centreon.com/current/en/administration/secure-platform.html (Centreon), https://docs.centreon.com/current/en/graph-views/secure-your-map-platform.html (Map) and update to the latest version 20.10, https://docs.centreon.com/current/en/update/update-centreon-platform.html

6 Partition your network

Make sure that you have tightened the security of your servers before exposing them to the Internet. The Centreon server must never be front-end with the Internet and must be protected / partitioned by intermediate mechanisms - at least a reverse proxy and a WAF (Web Application Firewall).

The flows must be encrypted and the use of the TLS client certificate is strongly recommended.

We recommend that you follow the ANSSI guide available here:
https://www.ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/

Be aware that in order to benefit from specific Centreon services, your local Centreon platform must communicate with Centreon Cloud Services Endpoints.

These services allow you to have:
- CEIP (Customer Experience Improvement Program)
- active licences
- Enterprise Plugin Packs
- AI/ML services (beta)
- Proactive Support (beta)
- Yum repositories (for install/update RPM packages).

You must thus allow only the following endpoints through your proxy and firewalls:
- https://statistics.centreon.com
- https://api.imp.centreon.com
- https://api.a.prod.mycentreon.com
- https://api.a.prod.mycentreon.com

All these endpoints are using HTTPS protocol.

7 Monitor the platform integrity

Whether it is the hardware part or the software part, monitor the integrity of your platform. Different tools are at your disposal including Ossec, Wazuh or for a more autonomous use, Tripwire and Aide.

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

These tools will allow you, among other things, to control file integrity by monitoring critical directories. Any addition or modification will be subject to an alert that you can process.

8 Backup and export event logs

Best practices recommend exporting logs and keeping them 3 months "live" (hot storage) and 1 year at rest (cold storage).

9   Going further

We think that open source code is safer by nature than proprietary code.

Like all open source software, you have access directly to the Centreon open source code hosted on GitHub public repositories (https://github.com/centreon). You can analyze, contribute, improve, and track code changes.

This code must be protected by your infrastructure. We can only recommend that you follow the best security practices. An interesting document is the guide of recommendations for the protection of essential information systems provided by ANSSI at this address: https://www.ssi.gouv.fr/guide/recommandations-pour-la-protection-des-systemes-dinformation-essentiels/