Pedro Ferreira Follow

May 3, 2021 · 2 min read · Listen

Save

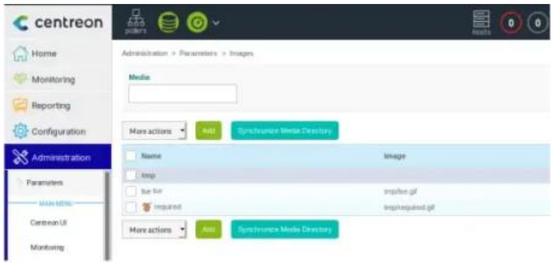
Vulnerability affecting some versions of centreon.

During my arduous journey to obtain OSCP certification, which happened in Nov/2020, I discovered a zero-day vulnerability in Centreon software, which made it possible to transfer files to the server through the application as if it were an image.

Below I will describe the steps tested in Centreon version 19.04.0:

Centreon's login page.

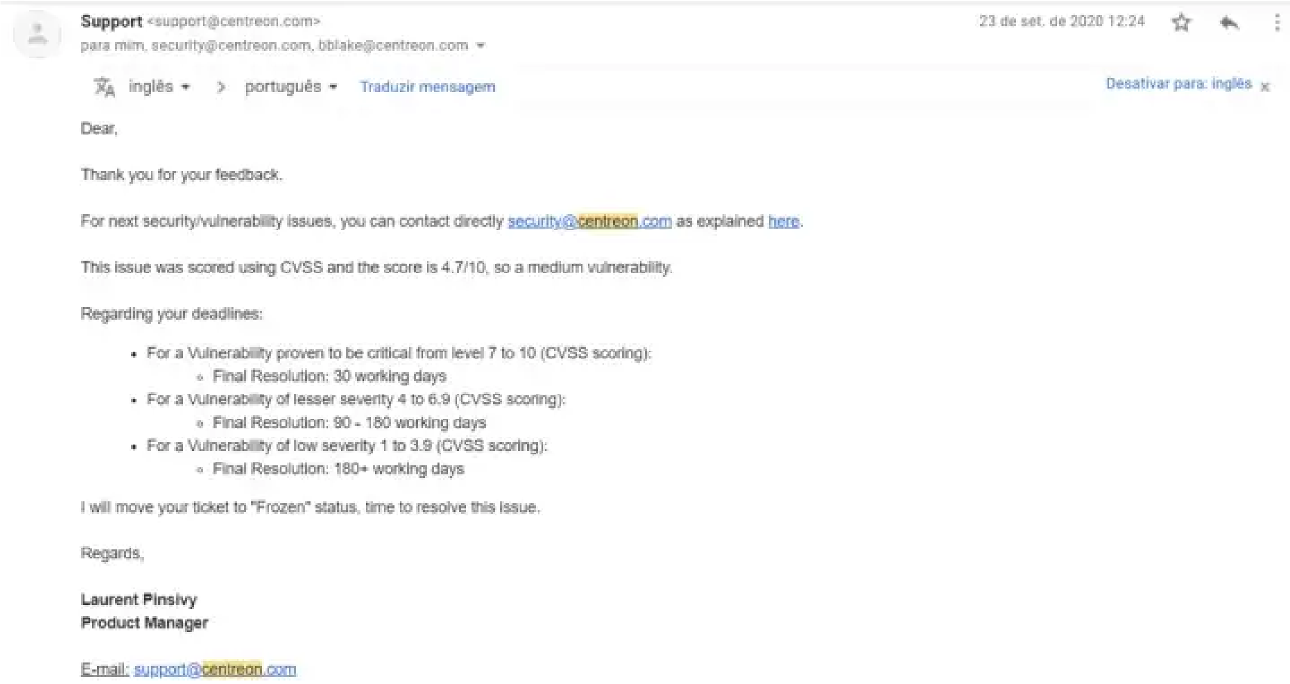
In the administration console, specifically in the Administration/Parameters/Images section, it is possible to rename any file to the gif extension and perform the upload without any further validation. Then, the files are available in the /usr/share/centreon/www/img/media/ folder:



lse.sh file uploaded to the server as lse.gif.

In this case, I had access to the server with a non-root user and the server did not have wget installed or other file transfer tools. So, I uploaded scripts and exploits by renaming them with the .gif extension and then went back to the normal extension when they were already on the server. This process can facilitate escalation of privileges.

After identifying the problem, I contacted Centreon's information security area and obtained the information that this vulnerability had been classified with a CVSS of 4.7, that is, a medium rating vulnerability:



Support <support@centreon.com>
para mim, security@centreon.com, bblake@centreon.com
23 de set. de 2020 12:24

Dear,

Thank you for your feedback.

For next security/vulnerability issues, you can contact directly security@centreon.com as explained here.

This issue was scored using CVSS and the score is 4.7/10, so a medium vulnerability.

Regarding your deadlines:

- For a Vulnerability proven to be critical from level 7 to 10 (CVSS scoring):
  - Final Resolution: 30 working days
- For a Vulnerability of lesser severity 4 to 6.9 (CVSS scoring):
  - Final Resolution: 90 - 180 working days
- For a Vulnerability of low severity 1 to 3.9 (CVSS scoring):
  - Final Resolution: 180+ working days

I will move your ticket to "Frozen" status, time to resolve this issue.

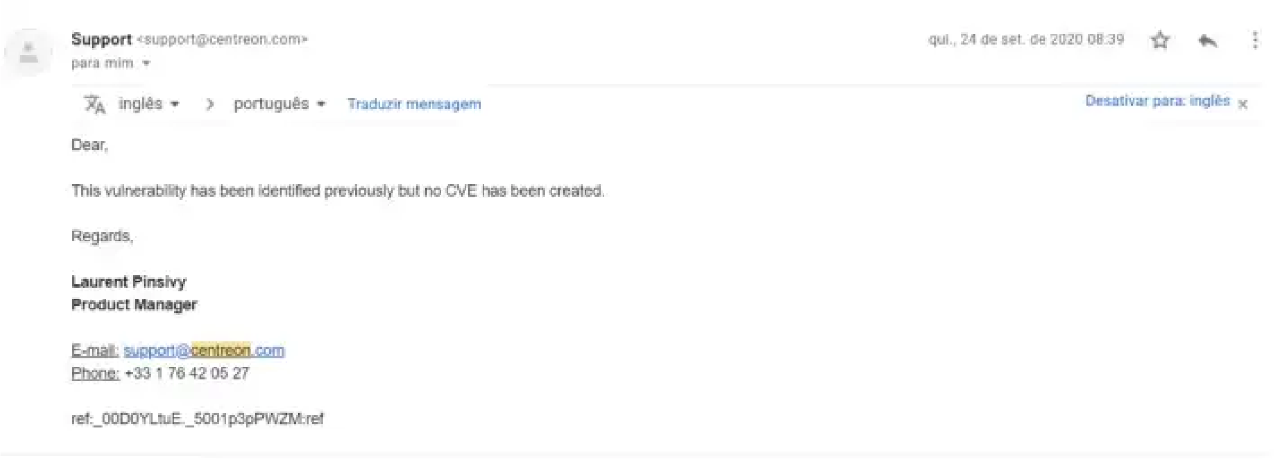
Regards,

Laurent Pinsivy
Product Manager

E-mail: support@centreon.com

Vulnerability classification by Centreon.

Also, I was informed that the vulnerability had been identified, but no CVE had been created:



Support <support@centreon.com>
para mim
qui., 24 de set. de 2020 08:39

Dear,

This vulnerability has been identified previously but no CVE has been created.

Regards,

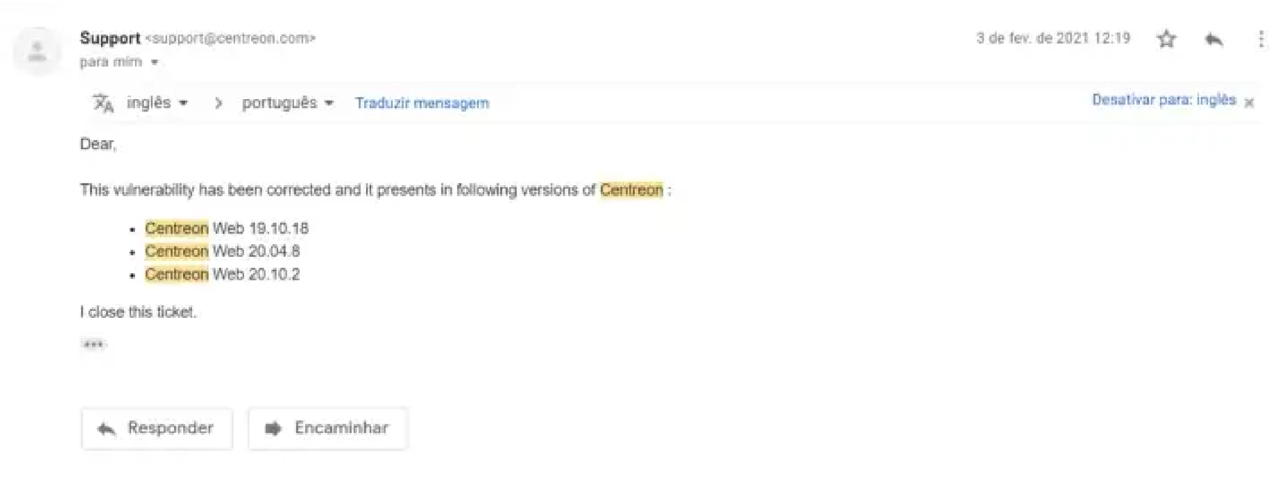
Laurent Pinsivy
Product Manager

E-mail: support@centreon.com
Phone: +33 1 76 42 05 27

ref:_00D0YLtuE._5001p3pPWZM:ref

No CVE created for this vulnerability.

Approximately 5 months later, I received a new email from Centreon stating that the vulnerability had been fixed, in addition to confirmation about the affected versions:



Support <support@centreon.com>
para mim
3 de fev. de 2021 12:19

Dear,

This vulnerability has been corrected and it presents in following versions of Centreon :

- Centreon Web 19.10.18
- Centreon Web 20.04.8
- Centreon Web 20.10.2

I close this ticket.

Vulnerability fixed.

Cyber Pentesting Hacking Centreon Vulnerability