Telecom Systems SA
Ch. de Budron E7
Case Postale 468
1052 Le Mont sur Lausanne
https://www.telsys.ch

TS News

CENTREON PROVIDES CLARIFICATIONS FOLLOWING THE PUBLICATION OF THE ANSSI REPORT.

18 February, 2021

*The attack concerns an obsolete open source version of the software, deployed without complying with the confidentiality recommendations of the **ANSSI** **(National Agency for the Security of Information Systems).***

Centreon clients are not concerned.

Centreon, a trusted partner for the operational excellence of information systems, provides clarifications following the publication of **ANSSI's CERTFR-2021-CTI-004 report.**

ANSSI published yesterday, February 15, a report on a supposed security flaw in the **Centreon** supervision software platform. This report could lead one to believe that the solutions marketed by **Centreon** would present security flaws. This press release specifies **Centreon's** position in the light of current knowledge concerning the identified campaign and its exchanges with the **ANSSI**.
Centreon calls, moreover, the companies and public organisations to respect the rules of computer security and to use preferably the updated and supported versions of its solutions.
Centreon would like to make some important clarifications:

LACK OF INFORMATION SECURITY:

The attack described by **ANSSI** concerns exclusively 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. Not only has this version not been supported for more than 5 years, but it also seems that it has been deployed without respect for the security of servers and networks, in particular connections to the outside of the entities concerned. Since this version, **Centreon** has **published 8 major versions**. **Centreon** reminds the importance of the respect of the good practices of computer security and of the recommendations of installation and security of the **ANSSI software**.

https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

Telecom Systems SA
Ch. de Budron E7
Case Postale 468
1052 Le Mont sur Lausanne
https://www.telsys.ch

NO CUSTOMERS IMPACTED:

According to the exchanges of the last 24 hours with the ANSSI, no Centreon client has been impacted. The ANSSI specifies that only about fifteen entities have been the target of this campaign, and that they are all users of an obsolete open source version (v2.5.2), which has not been supported for 5 years. Centreon is currently contacting all its clients and partners to accompany them towards a VE.

NO SPREAD OF MALICIOUS CODE:

The **ANSSI** report and our exchanges with them confirm that **Centreon** did not distribute or contribute to the spread of 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.

FINISHED CAMPAIGN:

Moreover, **ANSSI** specifies that the campaign in question is over and that no malicious activity is to be observed at present.

RECOMMENDATION:

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

About Centreon:

Centreon *delivers a business centric IT supervision software platform for the operational excellence of IS. Complete and integrating the latest advances in predictive artificial intelligence, it is designed for today's complex, distributed,* ***Multi-Cloud infrastructures*** *. More information on www.centreon.com .*