Cybersécurité : des attaques visent les supercalculateurs en Europe

Assiste-t-on à une opération cybercriminelle d'envergure ciblant les supercalculateurs ?

De nombreuses institutions académiques européennes ont rapporté, ces derniers jours, des incidents de sécurité dans ce sens.

L'université d'Édimbourg avait donné l'alerte lundi 11 mai. À la suite d'accès indésirables sur son superordinateur ARCHER, elle l'a isolé du réseau. Il est question d'un problème « sévère » qui nécessitera entre autres d'invalider tous les mots de passe et clés SSH.

Ce même jour, le groupement allemand bwHPC a fait état de la coupure forcée de plusieurs systèmes dans le land du Bade-Wurtemberg :

- bwUniCluster 2.0 et ForHLR II à l'Institut de technologie de Karlsruhe
- bwforCluster JUSTUS (supercalculateur dédié à la chimie et aux sciences quantiques) à l'université d'Ulm
- bwForCluster BinAC (bioinformatique) à l'université de Tubingue
- Hawk à l'université de Stuttgart

Mercredi 13, le chercheur en sécurité Felix von Leitner évoquait de probables incidents à Barcelone.

Il mettait aussi, sur la liste des victimes, le Centre de recherche de Juliers (Rhénanie-du-Nord-Westphalie)… qui allait confirmer le lendemain. Trois de ses systèmes (JURECA, JUDAC et JUWELS) sont indisponibles.

Autres victimes en Allemagne :

- Le Leibniz Rechenzentrum.
  Utilisé à la fois par l'Académie bavaroise des sciences et l'université de Munich, il a fermé l'accès à tous ses supercalculateurs depuis l'extérieur.
- L'université de Dresde et son superordinateur Taurus.

Un cryptomineur et rien de plus ?

L'université Louis-et-Maximilien de Munich est également touchée, à en croire Robert Helling.

Ce physicien a analysé les traces que l'attaque semble laisser sur les machines infectées. En l'occurrence, plusieurs fichiers localisés dans le dossier de polices de caractères /etc/fonts et disposant des droits root.

D'après l'EGI (European Grid Infrastructure), ces fichiers cachent un programme de minage de la cryptomonnaie Monero.

L'organe chargé de la coordination de la grille de calcul européenne ne parle pas d'un, mais de

deux incidents, « peut-être liés ».
D'un côté, celui dont Robert Helling se fait l'écho. De l'autre, une attaque impliquant également un mineur de Monero et qui a fait des victimes en Amérique du Nord comme en Chine.

L'entreprise américaine Cado Security estime que l'une et l'autre attaque reposent sur des identifiants SSH volés. Vraisemblablement sur des réseaux en Pologne (université de Cracovie) et en Chine (université Jiao-tong de Shanghai).

L'exploit utilisé pour passer en root semble impliquer la faille CVE-2019-15666. Elle est présente dans le noyau Linux, jusqu'à la version 5.0.19. Le souci : une mauvaise validation de répertoire qui peut entraîner un accès hors limites.

Le Centre suisse de calcul scientifique s'est lui aussi déclaré victime. Tout en assurant que les prévisions météo, réalisées en interne, ne seraient pas affectées.

Photo d'illustration © Carlos Jones/ORNL / licence CC by 2.0