Des pirates américains pourraient s'attaquer aux conduites d'eau et de gaz

Prendre le contrôle d'usines de retraitement d'eau, de pipelines de gaz voire de certains réseaux de centrales nucléaires, voilà le type de risques liés à des failles qu'ont découverts des experts de Core Security basé à Boston.

L'information révélée par l'agence de presse AP peut faire froid dans le dos même si rien ne prouve encore que quelqu'un ait pu utiliser ces vulnérabilités. Les sites visés sont des pipelines de gaz naturel au Chili, des mines de diamant et de cuivre en Australie ou encore des usines de retraitement d'eau en Louisiane ainsi qu'en Caroline du Nord.

Au centre de la controverse, la société Citect et son système de protection CitectSCADA. Des failles dans ses barrières de sécurité auraient été décelés, il y a plusieurs mois. **La société, filiale de l'équipementier énergétique Schneider Electric a réalisé un patch cinq mois seulement après la notification** des chercheurs de Core. Peut être un peu tard, une exploitation pourrait intervenir du fait que tous les clients n'ont pas encore installé le patch correctif.

Les experts de Core vont plus loin. Des hackers pourraient couper le courant de villes entières ou même empoisonner l'eau en déconnectant les systèmes de traitement de l'eau potable. Des risques grandissant qui vont de pair avec l'augmentation du nombre de machines et de systèmes reliés au Net. Pour preuve, Ivan Arce, responsable en chef du département Sécurité de Core estime que ce type de risque n'est désormais plus inévitable : « *Il ne s'agit pas d'un problème très élaboré. Si nous avons trouvé cette faille – qui, au passage, n'était pas difficile à démasquer – c'est qu'il doit être facile pour quelqu'un d'en faire autant* ».

Contacté, Schneider Electric n'a pas souhaité réagir à ces attaques sur ces failles de sécurité. Sa filiale, Citect a déjà conseillé à ses clients d'isoler leur système SCADA du Net ou de sécuriser leurs firewalls pour prévenir les systèmes des attaques du monde extérieur.