06/12/2013

EPR/18/013

www.enisa.europa.eu

L'Agence européenne de cybersécurité ENISA affirme qu'une meilleure protection des systèmes SCADA est nécessaire

Combien de temps encore pouvons-nous nous permettre d'utiliser des systèmes SCADA sans patchs, interroge l'Agence européenne de cybersécurité ENISA ? L'ENISA soutient que l'UE et ses Etats membres devraient respecter les procédures de gestion des correctifs (« patchs ») de façon proactive afin de renforcer la sécurité des systèmes SCADA.

La plupart des infrastructures critiques européennes concernent les secteurs de l'énergie, des transports et de l'approvisionnement en eau. Ces infrastructures sont principalement gérées et contrôlées par les systèmes SCADA (système d'acquisition et de contrôle des données), en tant que sous-catégorie des Systèmes de contrôle industriel (SCI). Durant la dernière décennie, la technologie SCADA, d'abord constituée de systèmes isolés, dispose désormais d'une architecture ouverte et de technologies standard fortement interconnectées avec d'autres réseaux d'entreprise ainsi qu'Internet.

- Une des conséquences de ces transformations est l'augmentation de la vulnérabilité face aux attaques extérieures. L'utilisation de patchs est un des moyens utilisés pour renforcer la sécurité des SCADA.
- Pour le moment, deux des plus importants problèmes concernant les techniques de correction sont le fort taux d'échecs des patchs (60%)[1] ou le manque de patchs ; moins de 50% des 364 vulnérabilités publiques bénéficiaient de patchs[2] pour protéger les SCADA.

Nous avons identifié un certain nombre de bonnes pratiques et recommandations pouvant améliorer le degré de sécurité des environnements SCADA en ce qui concerne les procédures de correction, dont nous voudrions faire mention ci-dessous :

- Les contrôles compensatoires :
  - Améliorer la défense en profondeur par la fragmentation des réseaux afin de créer des zones fiables qui communiquent en utilisant des contrôles d'accès ;
  - Renforcer les systèmes SCADA en retirant les caractéristiques non nécessaires ;
  - Utiliser des techniques telles que les listes blanches d'application (Application White Listing) et les inspections approfondies des paquets (Deep Packet Inspection).
- Les programmes de gestion des correctifs et les contrats de service :
  - Les détenteurs d'actifs devraient également établir des contrats de service de gestion des correctifs afin de définir la responsabilité des fournisseurs mais aussi des clients dans les processus de gestion de correctifs ;
  - Les détenteurs d'actifs devraient mener leurs propres tests. Ceci peut être fait de façon virtuelle ou en maintenant des systèmes de test séparés.
  - Les systèmes certifiés devraient être à nouveau certifiés après l'application d'un patch.

---

[1] *« En 2011, les SCI-CERT ont connu des taux d'échec de 60% des patchs corrigeant les vulnérabilités répertoriées pour les produits de système de contrôle ». (Kevin Hemsley –SCI-CERT)*

[2] *« Moins de 50% des 364 vulnérabilités publiques bénéficiaient de patchs (SCADA Security Scientific Symposium (S4), janvier 2012, McBride)*

Le directeur exécutif de l'ENISA, le professeur Udo Helmbrecht, fait remarquer que « *bien que les procédures de gestion de correctifs ne soient pas des remèdes miracles pour régler les problèmes de sécurité des systèmes SCADA, il est tout de même important que les organisations établissent une politique de gestion des correctifs. L'Union européenne ou les Etats membres pourraient sensibiliser davantage les acteurs quant à l'existence des patchs en appliquant les procédures de gestion des correctifs lorsque de nouvelles conditions sont imposées à la production d'appareils* ».

Voir le rapport complet

Contexte : Stratégie de l'UE en matière de cybersécurité,

Pour toute demande d'interview, veuillez consulter Ulf Bergström, porte-parole, ulf.bergstrom@enisa.europa.eu, téléphone portable : + 30 6948 460 143, ou notre expert, Adrian Pauna, resilience@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu