Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 21 août 2017
N° CERTFR-2017-ACT-033

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-033

1 - Risques liés à l'intégration des technologies du numérique dans les systèmes industriels

Les industries intègrent de plus en plus les nouvelles technologies à leur processus de production :
- IIoT (*Industrial Internet of Things*) ;
- applications mobiles ;
- utilisation de services dans le Cloud ;
- accès à distance pour le constructeur ;
- etc.

Ces ajouts peuvent augmenter la surface d'exposition des systèmes d'information. Les produits issus des nouvelles technologies ne suivent pas toujours des processus de développement aussi éprouvés que ceux des systèmes industriels.

La connexion d'équipements industriels à internet

Depuis quelques années, plusieurs cas d'attaques sur des systèmes industriels connectés à internet ont été recensés.

En juillet 2015, Charlie Miller et Chris Valasek montrent qu'il est possible de contrôler à distance une voiture alors qu'un conducteur est installé au volant.

En décembre 2015, l'attaque des infrastructures critiques du secteur énergétique ukrainien a été dévastatrice pour le pays. Les acteurs malveillants ont pu pénétrer les réseaux depuis internet.

Dans les cas où il n'est pas possible d'isoler physiquement le système d'internet, il est essentiel de sécuriser l'interconnexion. Dans ce cadre, un guide a été rédigé par l'ANSSI.

L'attaque utilisant le ver Stuxnet en 2010 sur les infrastructures iraniennes révèle qu'une isolation physique n'est pas suffisante pour protéger ses infrastructures critiques, cependant elle apporte une barrière supplémentaire à franchir pour un attaquant.

Cas des applications mobiles

De plus en plus d'éditeurs proposent des applications mobiles pour gérer des équipements industriels.

Les chercheurs en sécurité Alexander Bolshev et Ivan Yushkevich ont présenté en 2017 leurs travaux sur la sécurité de ces applications. Pour ce faire, ils ont analysé 32 applications disponibles sur le marché des applications Android et ont cherché des vulnérabilités à l'aide de la liste des 10 catégories de vulnérabilités les plus présentes dans les applications mobiles.

Leur étude met en avant un grand nombre de vulnérabilités, notamment dans les catégories suivantes :
- stockage des secrets sur l'équipement ;

– absence de chiffrement des communications ;
– cryptographie faible ;
– faible système d'authentification et d'autorisation ;
– absence de protection contre la modification du code.

Utiliser une telle application pour gérer des équipements industriels peut avoir des impacts désastreux en cas de compromission de celle-ci ou de l'équipement sur laquelle elle tourne.

Recommandations

Le CERT-FR recommande aux usagers et intégrateurs :
– de limiter et de sécuriser autant que possible les interconnexions entre internet et les systèmes industriels ;
– de s'assurer de la sécurité des applications tierces qui peuvent avoir un impact sur la sécurité de leurs systèmes.

Le CERT-FR recommande aux constructeurs et développeurs :
– d'intégrer la SSI dans leurs projets (par exemple en utilisant la méthode EBIOS.)

Documentation

– Guide de définition d'une architecture de passerelle d'interconnexion sécurisée :
https://www.ssi.gouv.fr/administration/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
– Lettre mensuelle n. 46 de l'Observation du Monde Cybernétique au sujet de la sécurité des véhicules connectés :
http://www.defense.gouv.fr/content/download/447223/7023420/file/OMC201601.pdf
– Lettre mensuelle n. 47 de l'Observation du Monde Cybernétique au sujet de la cyberattaque des réseaux électriques en Ukraine :
http://www.defense.gouv.fr/content/download/451231/7109792/file/OMC201602.pdf
– Hackers Remotely Kill a Jeep on the Highway - With Me in It :
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
– Cyber Attacks on Ukraine Power and Critical Infrastructure (vidéo) :
https://www.youtube.com/watch?v=lTwsDLO3C44
– La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) :
https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
– SCADA and Mobile in the IoT Age :
https://embedi.com/files/presentations/2017-confidence-scada-and-mobile-in-the-iot-age.pdf
– Mobile Top 10 2016 :
https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

2 - Rappel des avis émis

Dans la période du 14 au 20 août 2017, le CERT-FR a émis les publications suivantes :

– CERTFR-2017-AVI-265 : Vulnérabilité dans VMware NSX-V Edge
– CERTFR-2017-AVI-266 : Multiples vulnérabilités dans Citrix XenServer
– CERTFR-2017-AVI-267 : Multiples vulnérabilités dans le noyau Linux de RedHat
– CERTFR-2017-AVI-268 : Multiples vulnérabilités dans Xen
– CERTFR-2017-AVI-269 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2017-AVI-270 : Multiples vulnérabilités dans Drupal

Gestion détaillée du document

21 août 2017 version initiale.

22 août 2017 correction du lien SCADA and Mobile in the IoT Age.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2017-ACT-033