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 05 septembre 2016
N° CERTFR-2016-ACT-036

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-036

1 - Fuite de codes d'attaque attribués au groupe Equation

Le 13 août 2016, des attaquants se faisant appeler The Shadow Brokers ont publié un communiqué dans lequel ils affirment avoir récupéré des codes d'attaque associés au groupe Equation. Pour prouver leur crédibilité, ils ont mis à disposition deux archives chiffrées pour lesquelles la connaissance d'un mot de passe est nécessaire afin d'accéder au contenu. Seul un des deux mots de passe a été fourni, le second faisant l'objet d'une vente aux enchères.

Contenu de la première archive

Le premier fichier (`eqgrp-free-file.tar.xz.gpg`), pour lequel le mot de passe de déchiffrement a été communiqué, contient plusieurs codes ciblant principalement des équipements réseau.

Une fois déchiffrée puis décompressée, cette archive est composée d'un dossier nommé `Firewall` pesant 309,1 Mo et contenant 3639 fichiers, dont les horodatages varient de début 2009 à octobre 2013.

La collection d'outils, de scripts, d'exploits, de fichiers de configuration, d'implants et autres notices d'utilisation servent principalement à attaquer des pare-feux d'entreprise de grands constructeurs. Une liste exhaustive des outils contenus dans l'archive peut être trouvée ici[08], voire de manière plus étendue ici[09].

Les paragraphes suivants détaillent la situation pour les principaux équipementiers réseau concernés.

Cisco

Le 17 août, Cisco a réagi en publiant un billet ainsi que deux avis de sécurité, relayés dans l'alerte CERTFR-2016-ALE-005 du CERT-FR [01].
Les équipements impactés sont principalement les pare-feux PIX et Adaptive Security Appliance (ASA). Cisco a depuis fourni des correctifs de sécurité pour l'ensemble des vulnérabilités ciblées par les codes présents dans l'archive.

Parmi les codes disponibles, il est possible de mentionner :

EXTRABACON En exploitant la vulnérabilité CVE-2016-6366, il est possible d'effectuer un débordement de tampon qui permet une exécution de code à distance [02]. Il s'agit d'une faiblesse dans l'implémentation du protocole SNMP, quelle que soit la version de celui-ci. Cette faille est de type 0-jour et a donc été découverte par Cisco le 13 août. Jusqu'à cette date, l'exploitation de cette vulnérabilité n'avait probablement jamais été détectée. Cependant, certaines conditions spécifiques doivent être remplies pour que l'attaque réussisse : le service SNMP devait être activé sur l'interface ciblée et l'attaquant devait avoir le droit d'envoyer des paquets sur celle-ci. De plus, le nom de communauté (qui fait office de mot de passe) devait être connu. A noter qu'une société de sécurité hongroise a réussi à modifier l'attaque pour la faire fonctionner avec les versions les plus récentes d'ASA [03].

EPICBANANA La vulnérabilité CVE-2016-6367 avait été corrigée par Cisco en 2011. Lorsqu'un attaquant peut se connecter à un pare-feu vulnérable en telnet ou SSH, cet exploit lui permet d'élever ses privilèges sans connaître le mot de passe administrateur.

JETPLOW Contrairement aux deux codes mentionnés précédemment qui ne possèdent pas de fonctionnalité de persistance, le code JETPLOW permet de modifier le microgiciel d'un pare-feu afin de contourner les contrôles d'intégrité pour ainsi assurer la réinstallation du code EPICBANANA à chaque démarrage.

BENIGNCERTAIN Impactant les pare-feux PIX de version inférieure à 7.0, la vulnérabilité CVE-2016-1287 [04] concerne un possible débordement de tampon dans l'implémentation du protocole d'Internet Key Exchange (IKE). Avec un paquet IKE spécialement conçu, il est possible de faire fuiter des portions de la mémoire du pare-feu, en espérant récupérer ainsi des mots de passe ou des clés privées. Une attaque réussie a des implications énormes : en effet, l'attaquant est alors en mesure de déchiffrer les communications réputées protégées par un tunnel IPsec.

Fortinet

Le 17 août, Fortinet a également publié un avis de sécurité concernant une vulnérabilité dans le micrologiciel de ses pare-feux Fortigate [05]. Cette faille, identifiée depuis par CVE-2016-6909, a été corrigée silencieusement par Fortinet en août 2012. Le code `EGREGIOUSBLUNDER` exploitait cette vulnérabilité pour permettre à un attaquant de prendre le contrôle de l'équipement grâce à une requête HTTP malveillante exploitant une faille dans l'analyseur syntaxique des témoins de connexions (cookies).

Juniper Networks

Juniper a attendu le 19 août avant de communiquer [06]. S'ils reconnaissent que du code cible ScreenOS spécifiquement, ils affirment qu'aucun exploit à distance n'est inclus mais qu'ils continuent d'investiguer. Ils conseillent également de vérifier l'intégrité des images du micrologiciel contenu dans leur matériel [07].

Topsec

Plusieurs exploits ciblent le fabriquant chinois Topsec, mais celui-ci est resté silencieux.

Impact des codes

S'il est plus habituel de voir des attaques contre les postes utilisateurs, il n'est pas étonnant de constater que les équipements réseau sont également pris pour cibles. En effet, ceux-ci sont situés à des emplacements stratégiques, en périphérie ou au cœur même du réseau d'entreprise. De plus, si un attaquant arrive à compromettre du matériel censé assurer la sécurité périmétrique, il bénéficie alors d'un grande marge de manœuvre pour assurer sa propagation latérale au sein du réseau, d'autant plus si la sécurité n'a pas été pensée en profondeur.

Plusieurs constatations peuvent être formulées :

- Du code contenu dans l'archive cible fonctionne sur des équipements obsolètes encore utilisés aujourd'hui. Ils sont et resteront donc vulnérables jusqu'à leur remplacement ;
- Cette boîte à outils permet de couvrir à peu près toutes les phases d'une infiltration réseau, de la brèche initiale à l'établissement d'une tête de pont, du pivot latéral ou vertical au déchiffrement des communications protégées par un VPN.

L'impact de ces vulnérabilités peut varier en fonction des pratiques d'administration des équipements concernés ainsi que du durcissement des configurations déployées.

Recommandations

Le CERT-FR déconseille fortement l'utilisation de produits en fin de vie et invite à mettre à jour les produits encore maintenus afin de minimiser les risques d'exploitation d'une vulnérabilité.

De plus, appliquer le principe de défense en profondeur permet de réduire l'impact d'une intrusion lorsque celle-ci a lieu. Cela passe en premier lieu par une segmentation du réseau de l'entreprise. Ensuite, cela nécessite un durcissement de la configuration des divers équipements ainsi qu'une veille sur leur intégrité couplé à une maintenance régulière. Enfin, les efforts de sensibilisation des administrateurs et utilisateurs ne doivent pas être sous-estimés.

Dans le cadre spécifique à cette menace, les entreprises possédant ou ayant possédé du matériel vulnérable doivent commencer par remplacer ou mettre à jour les équipements ciblés lorsque ceci est possible. Ensuite, il faut considérer que les communications échangées ces dernières années ont potentiellement été compromises, ce qui implique non seulement de changer les secrets ayant permis de protéger ces communications mais également ceux (clés privées, mots de passe, etc.) ayant pu transiter sur ces liens.

Documentation

01 Bulletin d'alerte CERTFR-2016-ALE-005
http://www.cert.ssi.gouv.fr/site/CERTFR2016-ALE-005/index.html
02 Démo EXTRABACON
https://xorcat.net/2016/08/16/equationgroup-tool-leak-extrabacon-demo/
03 Tweet SilentSignal
https://twitter.com/SilentSignalHU/status/768095445444861952/photo/1
04 PIXPocket
https://musalbas.com/2016/08/18/equation-group-benigncertain.html
05 Avis CERTFR-2016-AVI-283
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-283/index.html
06 Annonce Juniper
https://forums.juniper.net/t5/Security-Incident-Response/Shadow-Brokers-Release-of-Hacking-Code/ba-p/296128
07 Avis Juniper
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10605
08 Equation Group Firewall Operations Catalogue
https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html
09 NSA's TAO Division Codewords
http://electrospaces.blogspot.fr/p/nsas-tao-division-codewords.html

2 - Sources de veille pour la sécurité des SCADA

Les systèmes industriels sont exposés à des risques de sécurité au même titre que les autres systèmes d'information. Depuis la révélation au public du ver *Stuxnet*, les constructeurs et la communauté s'appliquent à tester et améliorer la sécurité des différents équipements impliqués dans un système industriel.

Cet article vise à recenser les différentes sources de bulletins d'informations, correctifs, recommandations et documents de recherche associés à la sécurité des systèmes industriels et leurs protocoles. Cette liste n'est pas exhaustive et sera amenée à évoluer.

Liens

Sites du secteur public

- ICS-CERT :
https://ics-cert.us-cert.gov/ (en) - Alertes, recommandations, veille, rapports

Sites de constructeurs

- Belden :
https://www.belden.com/blog/industrialsecurity/index.cfm (en) - Articles, recommandations
- Rockwell Automation :
https://www.rockwellautomation.com/global/products-technologies/security-technology/overview.page?tab4 (en) - Recommandations
- Schneider Electric :
https://blog.schneider-electric.com/tag/cyber-security-tag/ (en) - Articles
- Schneider Electric :
http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cyber-security-vulnerabilities-sorted.page (en) - Vulnérabilités
- Siemens :
https://www.siemens.com/cert/en/cert-security-advisories.htm (en) - Vulnérabilités

Sites de chercheurs et sociétés de sécurité

- https://scadastrangelove.blogspot.com/ (en)
- https://scadahacker.com/ (en)

Conférences

- 4SIC (Stockholm, Suède) :
  https://4sics.se/
- CRITIS (Mondial) :
  http://www.critis2016.org
- ICS Cyber Security Conference (Atlanta, Georgie, USA) :
  http://www.icscybersecurityconference.com
- S4 (Miami, Floride, USA) :
  https://www.digitalbond.com/s4/

3 - Rappel des avis émis

Dans la période du 29 août au 04 septembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-289 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-290 : Vulnérabilité dans Adobe ColdFusion
- CERTFR-2016-AVI-291 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

05 septembre 2016 version initiale.