Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Affaire suivie par Frédéric PERRIOT

Paris, le 05 DEC. 2016
N° 5037 /ANSSI/COSSI/DTO/BFS

Le directeur général
de l'agence nationale de la sécurité des systèmes d'information
à
destinataires *in fine*

Objet : Actions de prévention et de réaction suite aux révélations SHADOW BROKERS.

Annexe : Détails des vulnérabilités par équipements concernés (page 3 à 5).

1 Contexte

Le 13 août 2016, un groupe se faisant appeler SHADOW BROKERS a publié un ensemble d'outils d'attaque informatique hautement sophistiqués. Cet ensemble est présenté comme appartenant à un mode opératoire dénommé EQUATION GROUP.

Utilisés à des fins d'espionnage, les outils publiés comprennent des codes d'exploitation de failles présentes sur différentes marques de pare-feu. Parmi les failles révélées, certaines étaient inconnues et ont fait l'objet de correctifs récents par les éditeurs.

En outre, les publications de SHADOW BROKERS révèlent l'existence d'implants micro-logiciels (*firmware*) susceptibles d'être installés non seulement par les codes d'exploitation de vulnérabilités cités plus haut, mais également par le biais d'une interception physique des matériels lors de leur livraison.

Depuis cette publication, des codes fonctionnels permettant de prendre le contrôle à distance d'équipements réseau ou d'en soutirer des données confidentielles sont disponibles publiquement. Ils sont accessibles à tous les attaquants et ne nécessitent pas de compétences élevées pour être utilisés.

2 Prévention

Afin de réduire les risques de compromission, il convient, conformément à la Politique de sécurité des systèmes d'information de l'Etat (PSSIE), de sécuriser l'accès physique aux équipements réseau ainsi que leurs locaux et de durcir la configuration des périphériques. En particulier, il apparaît nécessaire de :

- désactiver les services inutiles ;
- changer les identifiants et les mots de passe par défaut des équipements ;
- utiliser des mots de passe complexes et les renouveler régulièrement ;
- filtrer les connexions aux interfaces d'administration ;
- sur les équipements supportés, activer le démarrage sécurisé (*Secure Boot*) ;
- journaliser les événements.

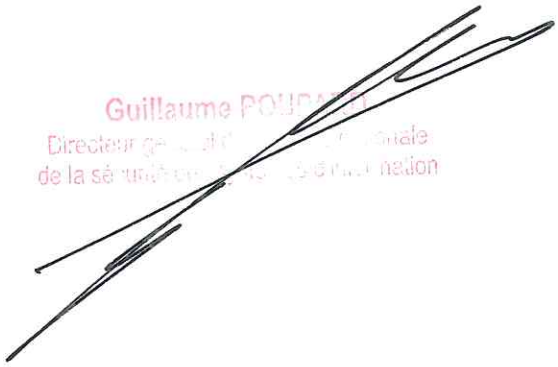
Il convient de maîtriser les équipements réseau exploités, notamment le système d'exploitation installés sur ces équipements :

- ils doivent provenir directement du constructeur, pas d'un réseau pair-à-pair ou d'un site non officiel ;
- leur intégrité doit être vérifiée, avant installation et périodiquement après, selon le guide du constructeur ;
- les modifications de leur configuration doivent être maîtrisées et contrôlées ;
- les mises à jour de sécurité doivent être appliquées dans les meilleurs délais après publication.

3 Recherches de compromission

L'agence nationale de la sécurité des systèmes d'information (ANSSI) recommande aux ministères de contrôler au plus tôt l'intégrité des équipements identifiés en annexe, en s'appuyant sur les guides techniques constructeur référencés et d'appliquer les correctifs disponibles.

En cas de suspicion de compromission, des analyses pourront être réalisées par l'ANSSI afin de vérifier l'intégrité des équipements.



Annexe

Détails des vulnérabilités par équipements concernés

1 Publications du CERT-FR

Les vulnérabilités révélées par la fuite SHADOW BROKERS ont suscité plusieurs alertes du CERT-FR :

- CERTFR-2016-ALE-005 du 18 août 2016, portant sur deux vulnérabilités dans les pare-feu *CISCO* ASA et PIX, permettant d'en prendre le contrôle à distance (alerte close le 5 septembre, suite à la publication des correctifs par *CISCO*).
- CERTFR-2016-ALE-007 du 19 septembre 2016, portant sur une vulnérabilité de type fuite mémoire dans les pare-feu *CISCO* fonctionnant sous IOS.

Outre ces alertes, le bulletin d'actualité CERTFR-2016-ACT-036 synthétise le contenu de l'archive des codes SHADOW BROKERS.

2 Listes des vulnérabilités et produits affectés

2.1 Produits *CISCO*

a CVE-2016-6366

La **CVE-2016-6366** est une faille de corruption mémoire permettant une exécution de code arbitraire à distance sur les pare-feu *CISCO* ASA et PIX. L'exploit EXTRABACON révélé par SHADOW BROKERS utilise cette vulnérabilité pour désactiver la vérification de mot de passe par les systèmes vulnérables.

Cette vulnérabilité fait l'objet de l'alerte CERTFR-2016-ALE-005.

Produits affectés :

- *CISCO* ASA 5500 Series Adaptive Security Appliances;
- *CISCO* ASA 5500-X Series Next-Generation Firewalls;
- *CISCO* ASA Services Module pour *CISCO* Catalyst 6500 Series Switches et Cisco 7600 Series Routers ;
- *CISCO* ASA 1000V Cloud Firewall ;
- *CISCO* Adaptive Security Virtual Appliance (ASAv);
- *CISCO* Firepower 9300 ASA Security Module ;
- *CISCO* PIX Firewalls ;
- *CISCO* Firewall Services Module (FWSM);
- *CISCO* Firepower 4100 Series ;
- *CISCO* Firepower Threat Defense Software ;
- *CISCO* Industrial Security Appliance 3000.

Liens :

http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-005/index.html

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

b *CVE-2016-6367*

La **CVE-2016-6367** est une faille de corruption mémoire permettant une élévation de privilèges depuis la ligne de commande des pare-feu Cisco ASA et PIX. L'exploit EPICBANANA révélé par SHADOW BROKERS emploie cette faille pour contourner la vérification du mot de passe administrateur sur les systèmes vulnérables.

Cette vulnérabilité fait l'objet de l'alerte CERTFR-2016-ALE-005.

Liens :

http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-005/index.html

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

c *CVE-2016-6415*

La **CVE-2016-6415** est une fuite mémoire présente dans plusieurs versions du système *CISCO* IOS. L'exploit BENIGNCERTAIN révélé par SHADOW BROKERS utilise cette vulnérabilité pour lire la mémoire d'équipements *CISCO* vulnérables.

Cette vulnérabilité fait l'objet de l'alerte CERTFR-2016-ALE-007.

Produits affectés :

- *CISCO* IOS XR versions 4.3.x ;
- *CISCO* IOS XR versions 5.0.x ;
- *CISCO* IOS XR versions 5.1.x ;
- *CISCO* IOS XR versions 5.2.x ;
- *CISCO* IOS XE toutes versions ;
- *CISCO* IOS, voir sur le site du constructeur pour vérifier si votre système est vulnérable (cf. section Documentation).

Liens :

http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-007/CERTFR-2016-ALE-007.html

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

Guides *CISCO* sur le contrôle d'intégrité :

L'ANSSI recommande aux ministères de contrôler au plus tôt l'intégrité de leurs équipements, puis d'appliquer les correctifs disponibles.

http://www.cisco.com/c/en/us/about/security-center/integrity-assurance.html

http://www.cisco.com/c/en/us/about/security-center/asa-integrity-assurance.html

2.2 Produits *FORTINET*

La **CVE-2016-6909** est une faille de corruption mémoire affectant les pare-feu FORTIGATE. L'exploit

EGREGIOUSBLUNDER révélé par SHADOW BROKERS utilise cette vulnérabilité pour prendre le contrôle des systèmes vulnérables.

Produits affectés :

- FORTIGATE (FOS) versions antérieures à 4.3.9

Liens :

http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-283/CERTFR-2016-AVI-283.html

http://fortiguard.com/advisory/FG-IR-16-023

2.3 Produits *JUNIPER*

La fuite SHADOW BROKERS ne contient pas de code exploitant de vulnérabilité dans les produits *JUNIPER*, mais témoigne de l'existence d'implants spécifiques à ces produits, en particulier ceux tournant sous *ScreenOS*. Par conséquent, il est conseillé de mettre à jour les équipements *JUNIPER*.

Produits affectés :

- *ScreenOS* versions 5.0.0r0 à 6.3.0r13

Liens :

https://forums.juniper.net/t5/Security-Incident-Response/Shadow-Brokers-Release-of-Hacking-Code/ba-p/296128

2.4 Produits *RAPIDSTREAM* (*WATCHGUARD*)

La fuite SHADOW BROKERS révèle l'existence d'un code d'exploitation permettant une élévation de privilège locale sur les pare-feu *RAPIDSTREAM*. Les matériels vulnérables sont d'anciens modèles datant d'avant l'acquisition de la firme *RAPIDSTREAM* par *WATCHGUARD*, en 2002. Les produits *WATCHGUARD* plus récents ne sont a priori pas concernés. Néanmoins, il est conseillé de mettre à jour les équipements *WATCHGUARD*.

2.5 Produits *TOPSEC*

La fuite SHADOW BROKERS révèle l'existence de plusieurs failles dans les matériels du fabricant chinois *TOPSEC*, et contient quatre codes d'exploitation permettant d'en prendre le contrôle. Les révélations n'ont pas donné lieu à publication d'avis de sécurité par *TOPSEC*.

Si des ministères possèdent de tels matériels, ils doivent prendre contact avec l'ANSSI.

Destinataires

Présidence de la République

Monsieur Mathieu MALAISE, responsable de la sécurité des systèmes d'information.

Premier ministre

Monsieur Nicolas MOREAU, fonctionnaire de sécurité des systèmes d'information.

Monsieur Alain LEMAINAIS, responsable de la sécurité des systèmes d'information de la direction de l'information légale et administrative

Monsieur Laurent VOILLOT, responsable de la sécurité des systèmes d'information de la direction interministérielle des systèmes d'information et de communication de l'État.

Sénat

Monsieur Laurent LAURELUT, responsable de la sécurité des systèmes d'information.

Assemblée Nationale

Monsieur Thiébaut MEYER, responsable de la sécurité des systèmes d'information.

Ministère des affaires étrangères et du développement international

Monsieur François-Xavier PERRIN, fonctionnaire de sécurité des systèmes d'information.

Monsieur Michel CAZENAVE, responsable de la sécurité des systèmes d'information.

Ministère de l'environnement, de l'énergie et de la mer

Monsieur Serge PHILIBEAU, fonctionnaire de sécurité des systèmes d'information.

Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche

Monsieur Benoît MOREAU, fonctionnaire de sécurité des systèmes d'information.

Ministère de la justice

Monsieur Stéphane DUBREUIL, fonctionnaire de sécurité des systèmes d'information.

Ministère de l'économie et des finances

Monsieur Jean-Philippe PAPILLON, fonctionnaire de sécurité des systèmes d'information.

Ministère des affaires sociales et de la santé
Ministère du travail, de l'emploi, et du dialogue social

Monsieur Philippe LOUDENOT, fonctionnaire de sécurité des systèmes d'information.

Ministère de la défense

ICA Eric JAEGER, fonctionnaire de sécurité des systèmes d'information.

COL Laurent MAIRE, officier central de lutte informatique défensive.

Ministère de l'intérieur

Monsieur Nicolas MARGUET, fonctionnaire de sécurité des systèmes d'information.

Ministère de la culture et de la communication

Madame Florence ESSELIN, fonctionnaire de sécurité des systèmes d'information.

Ministère de l'agriculture, l'agroalimentaire et de la forêt

Monsieur André ALIX, fonctionnaire de sécurité des systèmes d'information.