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 09 mai 2016
N° CERTFR-2016-ACT-019

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-019

1 - Le marketing des vulnérabilités

Depuis plusieurs années, le nombre de vulnérabilités rapportées augmente. Ceci est dû à l'intensification du travail de recherche en sécurité informatique ainsi qu'à un élargissement du nombre de produits disponibles. Depuis deux ans, un autre phénomène s'accélère : le marketing de ces vulnérabilités à travers des outils de communication modernes.

Le système des Common Vulnerabilities and Exposures (CVE)

La MITRE Corporation est une organisation à but non lucratif financée par plusieurs administrations du gouvernement américain. Depuis 1999, elle s'occupe notamment de recenser toutes les vulnérabilités connues relatives aux systèmes d'informations en maintenant la liste des Common Vulnerabilities and Exposures (CVE-List)[1]. Ce dictionnaire a pour but de fournir un identifiant unique à chaque vulnérabilité afin de faciliter les interactions entre les différents acteurs de la sécurité informatique.

Lorsqu'un chercheur trouve une vulnérabilité et qu'il souhaite la révéler de manière responsable, il peut effectuer une requête auprès de MITRE pour réserver un identifiant de CVE. Afin de réduire sa charge, Mitre alloue également des blocs d'identifiants à des autorités déléguées : les CVE Numbering Authorities (CNA)[2]. Celles-ci sont principalement de grands constructeurs de matériel et de logiciels informatiques qui attribuent des numéros de CVE aux vulnérabilités de leurs propres produits. Certaines entités tierces sont cependant habilités et peuvent servir d'intermédiaire en cas de problèmes de communication (CERT/CC...).

Lorsqu'une CVE est réservée, elle prend la forme suivante : CVE-YYYY-NNNN* où YYYY est l'année, NNNN un nombre arbitraire composé de quatre chiffres et (N)* est ajouté s'il est nécessaire d'enregistrer plus de dix-mille vulnérabilités par an. Le système des CVE est prévu pour être utilisé par des spécialistes et ne pas comporter plus d'informations que nécessaire.

Les CVE "nommées"

Le système des CVE possède de nombreux avantages, mais n'est pas particulièrement parlant. En effet, le numéro de la CVE-2014-0160 reste obscur. Pourtant, le nom HEARTBLEED[3] est lui encore relativement connu, même du grand public. Pour rappel, le 7 avril 2014, une vulnérabilité touchant certaines versions d'OpenSSL a été annoncée publiquement, en se dotant pour l'occasion d'un site internet ainsi que d'un logo[4]. Un manque de validation des données du client permettait à un attaquant de lire aléatoirement 64 Ko de mémoire d'un serveur, de manière répétable et indétectable[5]. Cela permettait de récupérer des éléments sensibles en clair tels que les mots de passe ou les clés privées. Une telle faille dans un logiciel libre massivement utilisé sur internet, couplé à la communication effectuée simultanément a permis de cristalliser l'attention, ne serait-ce qu'un moment, sur la fragilité de la sécurité des échanges sur la toile.

De manière similaire, la CVE 2014-6271 a été nommée SHELLSHOCK[6][7]. Cette vulnérabilité plus critique permettait une exécution de code à distance et était présente depuis la fin des années 80 dans bash. De plus, plusieurs variantes de l'attaque ont été trouvées et SHELLSHOCK recouvre aujourd'hui 6 identifiants de CVE.

Seulement quelques semaines plus tard, la vulnérabilité POODLE[8](CVE-2014-3566) a été publiée. Si elle permettait le déchiffrement des communications, les conditions d'exploitation étaient assez restrictives. En effet, seul l'ancien protocole SSL3.0 était affecté. Dans le cadre d'une attaque pratique, l'attaquant devait se trouver sur le même réseau que la victime pour espérer dégrader le niveau de chiffrement. Quelques semaines plus tard, une variante de l'attaque pouvait s'appliquer à quelques versions de TLS (le successeur de SSL)[9].

La vulnérabilité CVE-2015-0235, appelée GHOST[10], a été publiée en 2015 et est causée par un problème dans la bibliothèque `glibc`. Si elle est considérée comme critique par la National Vulnerability Database (NVD), plusieurs facteurs ont considérablement limité l'impact de cette vulnérabilité. D'abord, un correctif existait depuis 2013, mais n'avait pas été déployé sur les distributions à long terme de Linux. Par ailleurs, seul un nombre réduit d'applications permettaient de passer d'un simple déni de service à une exécution de code à distance.

Début janvier 2015, la vulnérabilité FREAK[11], concernait à nouveau certaines versions d'OpenSSL et était due au fait que certains navigateurs pouvaient accepter des tailles de clé réduites (512 bits pour RSA), un vestige de lois datant des années 1990 et interdisant l'utilisation de clés d'une taille supérieure en dehors des Etats-Unis. Un attaquant pouvait se glisser au milieu d'un début de connexion et tenter de faire accepter par les parties une clé d'une taille permettant de déchiffrer les communications par force brute.

En mai 2015 une vulnérabilité similaire est apparue : la vulnérabilité CVE-2015-4000, baptisée LOGJAM[12], impactait les implémentations du protocole TLS lors de l'échange de clé Diffie-Hellman (DHE). La cause venait une fois de plus des lois régulant l'exportation de la cryptographie américaine à la fin du siècle dernier, les conséquences permettaient là encore de forcer une dégradation de la taille des clés à 512 bits. Ce qui pouvait déboucher sur un déchiffrement des messages en cas d'attaque de l'intercepteur actif. Une attaque pouvait impacter l'intégrité et la confidentialité des données, ainsi que l'authentification des parties en présence ou encore la non-répudiation. Cependant, comme dans le cas de FREAK, ces attaques sont difficilement réalisables de manière massive à moins d'avoir la main sur le coeur de réseau. LOGJAM a également été promu à travers un site internet[13].

La vulnérabilité CVE-2015-3456 a aussi été publiée en mai 2015. Celle-ci fut appelée VENOM[14], sans doute car une exploitation réussie permettait d'injecter du code dans une machine hôte à partir d'une machine virtuelle. Si, le fait de pouvoir sortir du confinement d'une machine virtuelle, est rare et pose de sérieux problèmes de sécurité, la vulnérabilité CVE-2015-3456 était limitée par plusieurs facteurs. En effet, elle n'est exploitable que sur un réseau local et à condition que l'attaquant ait obtenu les droits administrateurs dans la machine invitée. Cependant, VENOM peut fonctionner indépendamment du système d'exploitation virtualisé.

En fin juillet 2015, le système d'exploitation Android a été touché par la vulnérabilité nommée STAGEFRIGHT[15], dont le nom venait de la bibliothèque qui contenait la vulnérabilité CVE-2015-3827. Un attaquant pouvait prendre le contrôle d'un ordiphone vulnérable en envoyant un MMS contenant un fichier multimédia piégé, et ce sans aucune interaction de la part de l'utilisateur. STAGEFRIGHT a mis en lumière les faiblesses du modèle de mise à jour d'Android : Google apporte ses correctifs à l'Android Open source Project (AOSP). Chaque constructeur doit adapter ce code à ses propres produits, puis les opérateurs téléphoniques doivent effectuer des changements à leur surcouche logicielle. Depuis, Google a mis en place un cycle de mise à jour mensuel. Cependant en dehors de la gamme Nexus qui ne contient aucune surcouche logicielle (ni constructeur, ni opérateur), seuls les téléphones hauts de gamme les plus récents reçoivent dans certains cas les correctifs de sécurité.

Début 2016, DROWN[16] a été annoncée grâce à un site internet et d'un logo[17]. La vulnérabilité CVE-2016-0800 permettait de déchiffrer les communications entre un client et un serveur après avoir écouté plusieurs centaines de connexions. DROWN impactait principalement SSLv2, mais pouvait toucher TLS en cas d'utilisation des mêmes certificats.

Fin mars, des chercheurs allemands annonçaient BADLOCK[18] grâce à un site internet et un logo[19], sans aucun détail afin de piquer l'intérêt, comme de classiques campagnes de promotion. Les vulnérabilités CVE-2016-0128 (pour Windows) et CVE-2016-2118 (pour Samba) ont été révélées trois semaines plus tard. La vulnérabilité permettait une élévation de privilège mais nécessitait que l'attaquant soit déjà présent dans le réseau. Pour finir, on constate une différence entre le score de base Common Vulnerability Scoring System (CVSS), annoncé en version 3 de 7.1 (High) sur le site officiel[19] contre 5.9 (Medium) sur le site de la NVD (cf. lien dans le tableau ci-dessous). Pour précision, la NVD donne un score identique à BADLOCK, sur Windows et Samba.

Le 4 mai 2016, IMAGETRAGIK a été annoncé. Il s'agit de la vulnérabilité CVE-2016-3714 impactant ImageMagik, une bibliothèque de traitement d'images utilisée par les moteurs de plusieurs langages web (PHP, Ruby, Python). Celle-ci est triviale à exploiter et permet une exécution de code à distance. Cette bibliothèque n'est pas installée par défaut. IMAGETRAGICK dispose également d'un site internet ainsi que d'un logo[20], cependant ceux-ci n'ont pas été créés par les chercheurs ayant trouvé la vulnérabilité.

Pour résumer :

Nom	Identifiant CVE	CVSS v2	CVSS v3	lien NVD
HEARTBLEED https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160	CVE-2014-0160	5.0	–	
SHELLSHOCK https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271	CVE-2014-6271	10.	–	
POODLE https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566	CVE-2014-3566	4.3	3.1	
GHOST https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235	CVE-2015-0235	10.	–	
FREAK https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204	CVE-2015-0204	4.3	–	
LOGJAM https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000	CVE-2015-4000	4.3	3.7	
VENOM https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3456	CVE-2015-03456	7.7	–	
STAGEFRIGHT https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3827	CVE-2015-3827	9.3	–	
DROWN https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800	CVE-2016-0800	4.3	5.9	
BADLOCK https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0128	CVE-2016-0128	4.3	5.9	
IMAGETRAGICK https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3714	CVE-2016-3714	10.	8.4	

Une source ouverte aux promotions

Après avoir énuméré les vulnérabilités de ces dernières années, il convient de replacer les choses dans leur contexte. Selon la NVD, ont été enregistrées :

- en 2014, 7937 vulnérabilités dont 1919 jugées sévères (avec un score de base CVSSv2 supérieur à 7) ;
- en 2015, 6488 vulnérabilités dont 2408 jugées sévères.

Sur les onze alertes émises par le CERT-FR en 2014, seules trois d'entre elles ont concerné les vulnérabilités décrites dans la section précédente (HEARTBLEED, SHELLSHOCK et POODLE). En 2015, seule STAGEFRIGHT a figuré parmi les quinze alertes publiées par le CERT-FR. Les autres alertes du CERT-FR sur cette période concernent majoritairement des éditeurs disposant d'un marché important, à savoir Microsoft, Apple, Google, Adobe ou encore Oracle. Dans une alerte de l'US-CERT datant de mi-2015 sur les 30 vulnérabilités les plus exploitées[21], HEARTBLEED est la seule à apparaître dans la liste, la grande partie de autres étant des vulnérabilités antérieures à 2014.

Deux conclusions peuvent être identifiées :

- Le phénomène du marketing des vulnérabilités est étroitement lié au code en Source Ouverte. En effet, les grandes compagnies n'ont pas intérêt à sur-médiatiser les vulnérabilités dans leurs produits. Certes, celles-ci n'ignorent pas le problème et publient des avis de sécurité afin d'avertir leurs clients de manière responsable. Certaines, comme Microsoft et Google, proposent même des programmes rémunérés de chasse aux bogues. Du côté des chercheurs, il est aussi plus simple de rechercher des vulnérabilités dans un code en source ouverte afin d'économiser l'ingénierie à rebours. Par ailleurs, les chercheurs s'exposent moins à d'éventuelles poursuites pour violation de propriété intellectuelle.

- Un décalage entre la médiatisation et le niveau d'impact émerge : une marque apposée autour d'une vulnérabilité, facilite la communication autour de celle-ci et de ses découvreurs. La renommée n'est cependant pas synonyme de criticité. Dans les milliers de vulnérabilités découvertes chaque année, de bonnes raisons doivent conduire à en faire sortir certaines du lot. Par exemple la vulnérabilité CVE-2016-1019[22], publiée début 2016, a fait plus de dégâts que DROWN ou BADLOCK. Les sites internet et les logos dédiés à des vulnérabilités ont l'intérêt de faire parler d'eux, donc de contribuer à élever la conscience générale sur les bonnes pratiques d'hygiène informatique. Cependant, il existe un risque non négligeable d'attirer l'attention sur les problèmes qui ne sont pas les plus importants. Par effet contraire, un message trop souvent répété conduira à le diluer, et à perdre ainsi l'oreille de décideurs qui commencent à être sensibilisés à ces sujets.

Le CERT-FR recommande l'application des correctifs de sécurité comblant les vulnérabilités, qu'elles soient nommées ou non, et ce dans les meilleurs délais afin de ne pas exposer les systèmes d'information de l'entreprise à des risques inutiles.

Documentation

01 CVE-LIST
http://cve.mitre.org/cve/index.html
02 liste CNA
http://cve.mitre.org/cve/cna.html
03 Bulletin d'actualité CERTFR-2014-ACT-015
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-015
04 Heartbleed
http://heartbleed.com/
05 Explication Heartbleed XKCD
https://xkcd.com/1354/
06 Bulletin d'actualité CERTFR-2014-ACT-039
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-039
07 Bulletin d'actualité CERTFR-2014-ACT-040
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-040
08 Bulletin d'actualité CERTFR-2014-ACT-042
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-042
09 Bulletin d'actualité CERTFR-2014-ACT-051
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-051
10 Bulletin d'actualité CERTFR-2015-ACT-005
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-005
11 Bulletin d'actualité CERTFR-2015-ACT-010
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-010
12 Bulletin d'actualité CERTFR-2015-ACT-025
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-025
13 Logjam
https://weakdh.org/
14 Bulletin d'actualité CERTFR-2015-ACT-023
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-023
15 Bulletin d'actualité CERTFR-2015-ACT-032
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-032
16 Bulletin d'actualité CERTFR-2016-ACT-010
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ACT-010
17 Drown
https://drownattack.com/
18 Bulletin d'actualité CERTFR-2016-ACT-016
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ACT-016
19 Badlock
http://badlock.org/
20 Imagetragick
https://imagetragick.com/
21 US-CERT Top 30 Targeted High Risk Vulnerablities
https://www.us-cert.gov/ncas/alerts/TA15-119A
22 Bulletin d'alerte CERTFR-2016-ALE-002
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-002

2 - Rappel des avis émis

Dans la période du 02 au 08 mai 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-149 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-150 : Multiples vulnérabilités dans Apple Xcode
- CERTFR-2016-AVI-151 : Multiples vulnérabilités dans OpenSSL
- CERTFR-2016-AVI-152 : Multiples vulnérabilités dans les produits Aruba
- CERTFR-2016-AVI-153 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-154 : Multiples vulnérabilités dans ImageMagick

Gestion détaillée du document

09 mai 2016 version initiale.

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-2016-ACT-019`