REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

Bulletin de sécurité N°1 du mois de Juin 2018

B.P. 6170 Tél : 22 08 64 98 Fax : 22 20 39 29 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN

Expression	Signification
Date de publication	Date à laquelle la vulnérabilité a été officiellement publiée par le développeur ou constructeur de la ressource concernée.
Dernière version	Lien de téléchargement de la dernière version de la ressource concernée, dans le cas d'une ressource logicielle ou système d'exploitation.
Description	Présentation des détails sur la vulnérabilité, entre autre les versions de la ressource concernée par la vulnérabilité, le vecteur d'exploitation de la vulnérabilité (local, réseau …).
Référence CVE	CVE (Common Vulnerabilities and Exposures) est un annuaire de vulnérabilités de sécurité. Cet annuaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro incrémenté). Plus d'information à l'adresse : http://cve.mitre.org/
Score CVSS	CVSS (Common Vulnerability Scoring System) est un système d'évaluation des vulnérabilités qui permet d'associer une valeur (comprise entre 0 et 10) évaluant la criticité d'une vulnérabilité. CVSS fournit un cadre commun pour évaluer les niveaux de criticité, les caractéristiques et les impacts des vulnérabilités de sécurité informatique. Plus d'informations à aux adresses : http://www.first.org/cvss/cvss-guide.html, http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/CVSSv2/
Solution	Lien vers d'éventuelles solutions permettant de colmater ou de contourner la vulnérabilité.
Vulnérabilité	Faille de sécurité publiée, Synopsis de la faille, généralement sur la forme « Vulnérabilité dans X » où X est une ressource informatique, matérielle, logicielle ou système d'exploitation concernée par la vulnérabilité.

II. Vulnérabilités publiées

II.1 Navigateurs

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome	Plusieurs vulnérabilités ont été corrigées dans Google Chrome. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont celles antérieures à 67.0.3396.79 pour Windows, Mac et Linux	08/06/2018	CVE-2018-6148	67.0.3396.79 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilités dans Mozilla Firefox	Une vulnérabilité a été corrigée dans Mozilla Firefox. Elle permet à un attaquant de provoquer une exécution de code arbitraire et un déni de service Les versions affectées sont les suivantes : Firefox versions antérieures à 60.0.2 Firefox ESR 52 antérieures à 52.8.1 Firefox ESR 60 antérieures à 60.0.2	07/06/2018	CVE-2018-0263	60.0.2 Télécharger	Mettre à jour le navigateur	8.4

II.2 Systèmes d'exploitation

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome OS	Google annonce des vulnérabilités non spécifiées sur Chrome OS versions antérieures à 67.0.3396.78 (Platform version: 10575.54.0)	08/06/2018	–	66.0.3359.170 Télécharger	Effectuez une mise à jour du système	9.0
Vulnérabilité dans le Noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données. Les versions infectées sont les suivantes : • Ubuntu 17.10 • Ubuntu 16.04 LTS • Ubuntu 18.04 LTS • Ubuntu 14.04 LTS • Ubuntu 12.04 ESM	12/06/2018	CVE-2018- 10940	18.04 LTS Télécharger	Effectuez une mise à jour du système	10.0

Vulnérabilité dans le Noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une élévation de privilèges. Les versions infectées sont les suivantes : • SUSE Linux Enterprise Live Patching 12-SP3	12/06/2018	CVE-2017- 13166	4.17-rc5 Télécharger	Effectuez une mise à jour du système	10.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Cisco	Plusieurs vulnérabilités ont été corrigées dans les produits Cisco. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.	07/06/2018	CVE-2018-0322	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-password-recoveryr	10.0
Vulnérabilité dans les produits Adobe Flash Player	Plusieurs vulnérabilités ont été corrigées dans Adobe Flash Player. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : Adobe Flash Player Desktop Runtime versions 29.0.0.171 Adobe Flash Player pour Google Chrome versions 29.0.0.171	08/07/2018	CVE-2018-5002	18.05 Télécharger	Effectuez une mise à jour	10.0

Vulnérabilité dans les produits F-SECURE	Une vulnérabilité a été corrigée dans les produits F-Secure. L'analyse d'un fichier RAR malicieusement conçue peut conduire à l'exécution de code arbitraire à distance. La vulnérabilité peut être exploitée à la fois localement pour obtenir une élévation de privilèges et à distance. Une attaque réussie permettra à l'attaquant de prendre le contrôle total du système.	07/06/2018	–	7.4 Télécharger	Veuillez-vous référer au bulletin de sécurité de F-SECURE https://www.f-secure.com/en/web/labs_global/fsc-2018-2	8.0
Vulnérabilité dans le produit VMware Horizon Client	Vmware a publié la correction d'une vulnérabilité affectant son produit VMware Horizon Client. L'exploitation de cette vulnérabilité peut permettre à un attaquant local l'élévation de privilèges. La version vulnérable est VMware Horizon Client versions antérieures à 4.8.0 sur Linux	01/06/2018	CVE-2018-6964	VMware Horizon 7 Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2018-0014.html	6.2
Vulnérabilité dans les produits Apple	Plusieurs vulnérabilités ont été corrigées dans les produits Apple. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et un déni de service à distance.	05/06/2018	CVE-2018-8897	Contacter Apple	Effectuez une mise à jour du système	10.0

Vulnérabilité dans les produits Asterisk	De multiples vulnérabilités ont été découvertes dans Asterisk. Elles permettent à un attaquant de provoquer un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Asterisk Open Source versions 13.x antérieures à 13.21.1 • Asterisk Open Source versions 14.x antérieures à 14.7.7 • Asterisk Open Source versions 15.x antérieures à 15.4.1 Certified • Asterisk version 13.18 antérieure à 13.18-cert4	12/06/2018	CVE-2018-12227	15.4.1 Télécharger	Veuillez-vous référer au bulletin de sécurité http://downloads.asterisk.org/pub/security/AST-2018-008.html	4.0

III. Actualités

1. L'ADN de millions de personnes à la merci des hackers

Les tests ADN consacrés à la recherche généalogique sont très à la mode, y compris en France. Malheureusement, la sécurité des données des utilisateurs n'est pas forcément à la hauteur des enjeux. L'une des entreprises du secteur, MyHeritage DNA, vient de révéler une énorme fuite de données. Les identifiants de 92 millions d'utilisateurs ont en effet été retrouvés quelque part « sur un serveur privé » par un chercheur en sécurité qui a alerté la société. Il est probable que des utilisateurs français soient également concernés par cet incident car les offres de MyHeritage sont également proposées en France, même si en théorie la vente de tests ADN est interdite dans notre pays

https://www.01net.com/actualites/l-adn-de-dizaines-de-millions-de-personnes-potentiellement-a-la-merci-de-hackers-1465180.html

2. Un PC Intel aussi petit qu'une carte de crédit

Le Compute Card d'Intel est un PC aux dimensions miniature. Il représente pourtant une solution tout à fait adaptée aux usages du quotidien : bureautique, multimédia et même jeu vidéo !

https://www.01net.com/mediaplayer/video/ce-pc-intel-est-aussi-petit-qu-une-carte-de-credit-1059501.html

3. IOS 12 Apple teste une fonction anti FBI

Disponible dès à présent en version beta, le nouveau système iOS 12 intègre une fonction de sécurité plutôt intéressante, mais qui n'a pas été mentionnée durant la keynote d'hier : l'USB Restricted Mode. Pour en profiter, il faut aller dans le menu « Face ID & Passcode » et activer l'option « UBS Accessories ». Dans ce cas, l'interface Lighting bloquera automatiquement toute communication USB si l'appareil n'a pas été déverrouillé depuis une heure.

https://www.01net.com/actualites/ios-12-apple-teste-une-fonction-anti-fbi-1464304.html

4. STEAM une faille vielle de dix ans qui permettait de faire planter des PC

Si vous êtes abonné à la plateforme de jeux Steam, peut-être avez-vous remarqué la mise à jour du logiciel client du 4 avril dernier. Elle a corrigé un mystérieux bug qui faisait planter le logiciel avec des paquets UDP malformés. Le chercheur qui a trouvé cette faille, Tom Court, vient maintenant de publier tous les détails techniques. Surprise : il s'avère que ce bug permettait en fait de prendre le contrôle du PC de n'importe quel utilisateur connecté, et cela pendant une période qui s'étend au moins de 2008 jusqu'en juillet 2017. Soit une dizaine d'années.

https://www.01net.com/actualites/steam-une-faille-vieille-de-10-ans-permettait-de-pirater-les-pc-des-gamers-1461032.html

5. On peut faire planter un PC avec un simple son…

Attention, le son peut nuire à la santé de votre ordinateur. Des chercheurs en sécurité des universités du Michigan et de Zhejiang ont découvert qu'il était possible d'altérer le fonctionnement d'un disque dur à plateau en le soumettant à des ondes acoustiques. Celles-ci peuvent faire chuter la vitesse de lecture, bloquer le disque en écriture, voire même crasher le système tout entier. Elles peuvent aussi provoquer des séquelles durables sous forme de secteurs endommagés, comme on peut le lire dans le papier scientifique.

https://www.01net.com/actualites/on-peut-faire-planter-un-pc-avec-un-simple-son-1459681.html

6. Le Kenya adopte une loi contre la pornographie sur la toile

En matière de cybercriminalité, le Kenya a récemment marqué un pas significatif dans la répression du phénomène. Le Parlement kenyan a en effet adopté une nouvelle loi sur la cybercriminalité qui condamne toute personne déclarée coupable de partage de pornographie juvénile par Internet d'une amende maximale de 20 millions de shillings, soit environ 111,3 millions de F Cfa ou d'une peine d'emprisonnement maximale de 25 ans.

https://www.ticmag.net/kenya-adopte-loi-contre-pornographie-internet/

IV. Malware : Top 10 du mois mai 2018 de Check Point

1 – **Coinhive** : Ce cheval de Troie est conçu pour effectuer l'extraction en ligne de la crypto-monnaie Monero lorsqu'un internaute visite une page Web. Le script java implanté utilise les ressources informatiques des utilisateurs finaux pour extraire de la monnaie cryptée.

2 – **Cryptoloot** : Ce malware utilise la puissance du processeur ou du GPU de la victime et les ressources existantes pour le crypto-mining, en ajoutant des transactions à la chaîne de blocage et en libérant de nouvelles devises. Similaire à Coinhive, ce programme est implanté sur des pages Web et utilise le pouvoir de traitement des internautes pour exploiter tous types de crypto-monnaies.

3 – **Roughted** : Campagne de publicité malveillante à grande échelle, elle est utilisée pour diffuser divers sites Web et charges embarquées malveillants tels que des escroqueries, des logiciels publicitaires, des kits d'exploitation de vulnérabilité et les logiciels de rançon. Il peut être utilisé pour attaquer n'importe quel type de plateforme et de système d'exploitation, et utilise le contournement des bloqueurs de publicités pour attaquer de la manière la plus efficace.

4 – **Necurs** : Ce botnet est l'un des plus actifs au monde, et on estime qu'en 2016, il comptait environ 6 millions de bots. Il propage de nombreuses variantes de logiciels malveillants, principalement des chevaux de Troie bancaires et des ransomwares.

5 – **JSEcoin** : Ce mineur JavaScript peut être intégré à n'importe quel site Web. JSEcoin permet de lancer un mineur directement dans le moteur de recherche en échange d'une navigation Web sans publicité.

6 – **Conficker** : Conficker est un ver informatique qui cible le système d'exploitation Windows. Il exploite les vulnérabilités de l'OS pour voler des données telles que des mots de passe. Ainsi, il prend le contrôle des ordinateurs touchés, les transformant en « zombie ». Les ordinateurs contrôlés forment alors un réseau, utile aux hackers.

7 – **Fireball** : Fireball est un logiciel publicitaire largement distribué par la société chinoise de marketing numérique Rafotech. C'est un détourneur de navigateur qui change le moteur de recherche par défaut et installe des pixels de suivi, mais qui peut aussi servir à télécharger des logiciels malveillants.

8 – **Dorkbot** : Dorkbot est un verre basé sur un IRC conçu pour permettre l'exécution de code à distance, ainsi que le téléchargement de logiciels malveillants vers le système déjà infecté. Ce dernier permet de voler des informations sensibles et de lancer des attaques par déni de service. Il installe un rootkit en mode utilisateur pour empêcher l'affichage ou l'altération des fichiers et modifie le registre pour s'assurer qu'il s'exécute chaque fois que le système démarre. Il enverra des messages à tous les contacts de l'utilisateur infecté, ou détournera un thread existant, pour diffuser un lien renvoyant vers la copie du verre.

9 – **Murofet** : Cheval de Troie qui cible la plate-forme Windows, ce logiciel malveillant est conçu pour implanter des fichiers malveillants supplémentaires dans un système déjà infecté. Il peut se propager via des spams et les fonctionnalités provenant d'autres logiciels malveillants.

10 – **Virut** : Virut est l'un des principaux distributeurs de botnets et de logiciels malveillants sur Internet. Il est utilisé lors d'attaques DDoS, de distribution de spam, de vol de données et de fraude. Ce malware se propage par le biais d'exécutables provenant de périphériques infectés, tels que des clés USB, ou via des sites Web compromis. Par ces biais, Virut modifie les fichiers hôtes locaux et ouvre une porte dérobée permettant de rejoindre un canal IRC contrôlé à distance par un hacker.

V. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses alerts@antic.cm et alerts@cirt.cm parmi vos contacts ou l'enregistrer comme expéditeur approuvé afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.
2. Ce document est produit régulièrement et téléchargeable sur notre site web www.cirt.cm . Vous y trouverez aussi des alertes et autres publications relatives à la cybersécurité et à la cybercriminalité.
3. Windows XP SP3 et Office 2003 ne sont plus supportés depuis le 8 avril 2014 par Microsoft. Si votre organisation n'a pas encore effectué une migration vers un poste de travail moderne, votre système d'information court de grands risques. En se basant sur les données des déploiements passés des clients Microsoft, le déploiement moyen en entreprise peut prendre de 18 à 32 mois. Pour plus d'informations :
   http://www.microsoft.com/fr-fr/windows/enterprise/fin-support-XP/default.aspx

   L'utilisation des solutions ne possédant aucun support technique présente un risque élevé étant donné qu'aucun correctif ne sera émis après d'éventuelles vulnérabilités détectées sur celles-ci.
4. HIDDEN COBRA - Cyberactivités nord-coréennes malveillantes : Le Département de la Sécurité Intérieure (DHS) et le Bureau Fédéral d'Investigation (FBI) ont identifié des activités malveillantes imputées au groupe dénommé HIDDEN COBRA, et ont fourni des détails techniques sur les outils et l'infrastructure utilisés par ces cyber-acteurs du gouvernement nord-coréen. Le but du partage de cette information est de sensibiliser les responsables des Systèmes d'Information sur la possibilité d'infection, et de réduire l'exposition à cette cyberactivité du gouvernement nord-coréen. Les outils de détection, et des solutions de prévention et d'éradication sont contenues dans les articles contenus dans la page suivante :
   https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
5. Afin de se prémunir au maximum d'éventuelle attaques informatiques pouvant endommager tout ou partie de vos systèmes, vous devez mettre à jour tous vos systèmes et logiciels utilisés. Nous vous recommandons donc de télécharger et d'installer toutes les dernières versions de logiciels et systèmes utilisés, uniquement sur les sites des constructeurs. Car tout logiciel téléchargé d'une source autre que celle du constructeur est potentiellement compromise par des malware et chevaux de Troie.

   Par ailleurs, si vous rencontrez quelques difficultés que ce soit dans l'application des correctifs susmentionnés ou ailleurs vous pouvez nous contacter à travers les adresses email alerts@antic.cm et alerts@cirt.cm ou au numéro de téléphone **242 09 91 64**.