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°2 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. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont celles antérieures à 67.0.3396.87.	08/06/2018	CVE-2018-6149	67.0.3396.87 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilités dans IE et EDGE	Plusieurs vulnérabilités ont été corrigées au niveau des deux navigateurs de Microsoft ; Internet Explorer et Edge. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire ou le contournement de la politique de sécurité.	13/06/2018	CVE-2018-8267	-	Effectuer une mise à jour via Windows Update	8.2

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	Plusieurs vulnérabilités ont été corrigées au niveau de plusieurs versions de Microsoft Windows. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire, l'élévation de privilèges, l'accès à des données confidentielles ou de causer un déni de service.	13/06/2018	CVE-2017-8233	Windows 10	Effectuer une mise à jour via Windows Update	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 un problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à la confidentialité des données. Les versions infectées sont les suivantes : • SUSE Linux Enterprise Live Patching 12-SP3	22/06/2018	CVE-2018- 12233	4.18-rc2 Télécharger	Effectuez une mise à jour du système	10.0

Vulnérabilité dans le Noyau Linux de RedHat	Redhat annonce la disponibilité d'une mise à jour de sécurité qui permet de corriger une vulnérabilité au niveau du noyau de plusieurs versions de Red Hat Enterprise Linux 7. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'accéder à des données confidentielles.	19/06/2018	CVE-2017- 3665	4.18-rc2 Télécharger	Effectuez une mise à jour du système	9.2

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 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.	21/06/2018	CVE-2018-0331	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-firepwr-pt	10.0
Vulnérabilité dans Microsoft Office	Plusieurs vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une divulgation d'informations, une élévation de privilèges, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	14/06/2018	CVE-2018-8254	-	Correctif disponible via Windows Upadte	7.3

Vulnérabilité dans Citrix XenServer	Une vulnérabilité a été corrigée dans Citrix XenServer. Un attaquant distant pourrait exploiter cette vulnérabilité pour accéder aux informations confidentielles. Les versions affectées sont les suivantes : XenServer 7.5 XenServer 7.1 LTSR Cumulative Update 1	19/06/2018	CVE-2018-3665	7.5 Télécharger	Effectuez une mise à jour du système	6.0
Vulnérabilités dans les Microprocesseurs Intel® Core	Une vulnérabilité surnommée ‘’Lazy FP State Restore’’ a été découverte dans les Microprocesseurs Intel® Core. L’exploitation de cette vulnérabilité peut permettre à un attaquant d’accéder aux informations confidentielles. Intel n'a pas encore publié de détails techniques sur la vulnérabilité, mais comme la vulnérabilité réside dans le processeur, la faille affecte tous les périphériques exécutant des microprocesseurs Intel Core indépendamment des systèmes d'exploitation installés.	14/06/2018	CVE-2018-3665	–	Correctif disponible via Windows Upadte	9.0

Vulnérabilité dans le produit VMware AirWatch	Vmware a publié la correction d'une vulnérabilité affectant sa solution de gestion de terminaux mobiles VMware AirWatch Agent. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant l'exécution de code arbitraire. La version vulnérable est VMware Horizon Client versions antérieures à 8.2 et 6.5.2 versions mobiles	13/06/2018	CVE-2018-6968	VMware AirWatch 8.2 Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2018-0015.html	6.2
Vulnérabilité dans phpMyAdmin	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. La version vulnérable est phpMyAdmin versions antérieures à 4.8.2.	25/06/2018	CVE-2018-8897	4.8.2 Télécharger	Effectuez une mise à jour du système	10.0
Vulnérabilité dans PHP	De multiples vulnérabilités ont été découvertes dans PHP. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • PHP versions 7.2.x antérieures à 7.2.7 • PHP versions 7.1.x antérieures à 7.1.19	22/06/2018	–	7.2.7 Télécharger	Effectuez une mise à jour du système	4.0

III. ACTUALITÉS

1. Firefox monitor l'outil qui va vous dire si vos comptes web sont compromis

Firefox s'apprête à lancer la phase de test de son prochain outil, Monitor, auprès de 250 000 utilisateurs. Un outil qui risque d'en intéresser plus d'un puisqu'il vous permettra de vérifier rapidement et en toute sécurité si des données liées à l'utilisation d'une de vos adresses mails pour vous connecter à votre compte mail, Twitter ou même votre service de livraison de courses à domicile préféré n'ont pas été piratées à votre insu lors d'une attaque ou de l'exploitation d'une brèche de sécurité.

https://www.01net.com/actualites/firefox-monitor-l-outil-qui-va-vous-dire-si-vos-comptes-web-sont-compromis-1478222.html

2. Un hacker a trouvé le moyen de bypasser tous les iPhones malgré les mots de passe

Mise à jour du 25 juin : Apple dément catégoriquement le hack effectué par Matthew Hickey... sans vraiment convaincre. Suite à la publication de la vidéo montrant le procédé, Apple a fait une déclaration pour le moins laconique à iMore : « Le récent rapport à propos du contournement du mot de passe sur un iPhone était une erreur, et le résultat d'un essai incorrect ». Mauvaise manipulation ou pas, le hacker a pourtant bel et bien réussi à y parvenir.
https://www.01net.com/actualites/ios-un-hacker-a-trouve-un-moyen-d-acceder-a-votre-iphone-malgre-votre-mot-de-passe-1476711.html

3. Google renforce la sécurité biométrique des smartphones sous Android

Quand on met tous ses œufs dans le même panier, on a tendance à vouloir s'assurer qu'ils y sont en sécurité. C'est un peu ce que nous faisons tous au quotidien avec nos smartphones. Nos contacts, nos échanges et autres communications, nos documents, tout se retrouve dans ces appareils qu'on promène avec nous mais risque à tout instant d'oublier, de perdre ou de se faire voler.

https://www.01net.com/actualites/google-renforce-la-securite-biometrique-des-smartphones-sous-android-o-et-p-1476651.html

4. Un Botnet peut rapporter plus de 20 millions de dollars par mois

Depuis plusieurs années, les réseaux de machines zombies sont devenus un pilier de l'activité cybercriminelle, tant pour distribuer du spam que pour générer des attaques DDoS ou frauder les systèmes bancaires ou publicitaires. Mais combien rapportent-ils ? Trois chercheurs de l'université néerlandaise de Twente viennent de publier une étude qui analyse le modèle économique du botnet et estime son potentiel de bénéfices. https://www.01net.com/actualites/un-

botnet-peut-rapporter-plus-de-20-millions-de-dollars-par-mois-1473558.html

5. Les USA envisagent des cybers frappes préventives contre leurs ennemis

Le message que veulent faire passer les Américains est clair : dans le cyberespace, la fête est bientôt finie. D'après The New York Times (NYT), le gouvernement des Etats-Unis veut passer à l'offensive et envisage désormais des cyber-frappes préventives dans les réseaux d'états étrangers pour contrer les cyber-combattants ennemis.

https://www.01net.com/actualites/les-etats-unis-envisagent-des-cyberfrappes-preventives-contre-leurs-ennemis-1473299.html

6. La douane Française démantèle une plateforme illégale

C'est une belle prise pour la douane française. Elle vient de mettre fin sur le Dark Web à un forum baptisé "Black Hand" (Main Noire) qui aurait compté plus de 3000 membres impliqués dans du trafic de données bancaires, d'armes, de stupéfiants ou encore de faux papiers. Le ministre de l'Action et des Comptes publics Gérald Darmanin s'est aussitôt félicité dans un communiqué de cette opération qui serait "une première du genre" en France et une vraie victoire contre "la cyberdélinquance".

https://www.01net.com/actualites/dark-web-la-douane-francaise-demantele-une-plateforme-illegale-1472191.html

7. L'application qui transforme les fans de football en mouchards

C'est une innovation qui pourrait inspirer de nombreuses ligues professionnelles de football. La Liga espagnole a décidé de pister les fans qui ont téléchargé son application mobile pour repérer les établissements qui diffuseraient ses matchs sans avoir payé. Une information révélée par le quotidien El Diaro. Nous avons donc téléchargé l'application pour savoir comment cela fonctionne.

https://www.01net.com/actualites/piratage-l-application-qui-transforme-les-fans-de-football-en-mouchards-1470130.html

8. Google solve update issue for Android App installed from unknown sources

Late last year, Google announced its plan to set up an automated mechanism to verify the authenticity of an app by adding a small amount of security metadata on top of each Android application package (in the APK Signing Block) distributed by its Play Store.

https://thehackernews.com/2018/06/google-play-store-app-updates.html

IV. 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**.