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 Janvier 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 Microsoft 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 l'accès à des données confidentielles.	10/01/2018	CVE-2018-0803	11 Télécharger	Veuillez-vous référer au guide de sécurité de Microsoft pour obtenir les nouvelles mises à jour https://portal.msrc.microsoft.com/en-us/security-guidance	8.1
Vulnérabilité dans Mozilla Firefox	Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant la correction d'une vulnérabilité au niveau de son navigateur Mozilla Firefox. L'exploitation de cette vulnérabilité peut permettre à un attaquant de créer une page web malicieuse pour accéder à des données confidentielles.	05/01/2018	CVE-2018-7845	57.0 Télécharger	Appliquer la dernière version	9.0

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 ou l'accès à des données confidentielles.	10/01/2018	CVE-2018-0753	Windows 10	Il est vivement recommandé de mettre à jour vos systèmes le plutôt possible.	9.3
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service à distance.	03/01/2018	CVE-2017-15845	8.0 Oreo Télécharger	-	8.0
Vulnérabilité dans le micrologiciel Intel pour Ubuntu	Une vulnérabilité a été découverte dans le microgiciel Intel pour Ubuntu. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : - Ubuntu 17.10 - Ubuntu 16.04 LTS	10/01/2018	CVE-2018-5715	17.10 Télécharger	Veuillez-vous référer au guide de sécurité d'Ubuntu pour obtenir les correctifs https://usn.ubuntu.com/usn/usn-3531-1/	

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 atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : - SUSE Linux Enterprise Software Development Kit 12-SP2 - SUSE Linux Enterprise Server 12-SP2 - SUSE Linux Enterprise High Availability 12-SP2	12/01/2018	CVE-2017-5754	4.15.rc7 Mettre à jour	Appliquer les correctifs inclus dans la nouvelle version	9.0
Vulnérabilité dans les produits Apple	Apple annonce la correction de la vulnérabilité « Spectre » qui a déjà fait l'objet d'un bulletin de sécurité et une alerte du CIRT. L'exploitation de cette vulnérabilité peut permettre à un attaquant de détruire l'isolation entre les différentes applications, ce qui permet à une application malveillante d'accéder aux données des autres applications. Les systèmes concernés sont les suivants : - Apple macOS High Sierra 10.13.2 - Apple iOS 11.2.2 - Apple safari 11.0.2 sur OS X El Capitan 10.11.6 et macOS Sierra 10.12.6	09/01/2018	CVE-2017-5715	Contacter Apple	Veuillez-vous référer au guide de sécurité d'Apple pour obtenir les correctifs https://support.apple.com/fr-ma/HT208397	9.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Flash Player	Adobe vient de publier des mises à jour qui permettent de corriger une vulnérabilité dans son produit Adobe Flash Player. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'accéder à des données confidentielles	10/01/2018	CVE-2018-4871	28.0.0.137 Télécharger	Télécharger la dernière version 28.0.0.137	5.0
Vulnérabilité dans les produits Vmware	Plusieurs vulnérabilités ont été corrigées dans les produits VMware. L'exploitation d'une de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire. Les systèmes infectés sont les suivants : - Fusion versions 10.x pour OS X antérieures à 10.1.1 - Workstation versions 14.x antérieures à 14.1.1	12/01/2018	CVE-2017-7525	Mettre à jour	Appliquer les patchs de sécurité	10.0

Vulnérabilité dans PHP	De multiples vulnérabilités ont été corrigées dans PHP. L'exploitation d'une de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire, l'accès à des données confidentielles ou le déni de service	12/01/2018	-	7.2.1 Télécharger	Télécharger la dernière version 7.2.1	7.8
Vulnérabilité dans Microsoft Office	Microsoft annonce la correction de plusieurs vulnérabilités au niveau de Microsoft Office. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire à distance.	12/01/2018	CVE-2018-819	-	Veuillez-vous référer au guide de sécurité de Microsoft Office pour obtenir les correctifs https://portal.msrc.microsoft.com/en-us/security-guidance	6.3

III. ACTUALITÉS

1. **Un nouveau malware sous macOS**

   L'année 2018 ne donnera aucun répit aux utilisateurs sous macOS. Le chercheur en sécurité Patrick Wardle vient de mettre la main sur « OSX/MaMi », un malware plutôt méchant qui traine actuellement sur la Toile. Un exemple d'infection a notamment été mentionné sur le forum de l'éditeur MalwareBytes. Le code malveillant est un exécutable 64-bit probablement diffusé par l'intermédiaire d'email ou de sites piégés. Une fois installé sur la machine, il modifie les paramètres DNS de l'ordinateur et installe un certificat racine bidon, ce qui permet à l'attaquant de déchiffrer et intercepter tous les échanges Internet de la victime. Bonjour les dégâts!
   http://www.01net.com/actualites/un-nouveau-malware-espionne-les-utilisateurs-sous-macos-1348748.html

2. **21% de baisse de performance sur les processeurs Intel**

   Les nuages s'accumulent sur le front de lutte anti-Meltdown et anti-Spectre. Alors que les premières mises à jour de microcode pour processeurs Intel arrivent enfin sur les ordinateurs Linux, le fabricant de puce américain a publié les résultats d'une première batterie de tests pour évaluer les baisses de performances. Quatre plateformes récentes *« totalement patchées »* ont été testées sous Windows 10 avec un disque SSD: Core i7 8700K (Coffee Lake), Core i7-8650U (Kaby Lake), Core i7-7920HQ (Kaby Lake) et Core i7-6700K (Skylake). Cette dernière a également été testée sous Windows 7, avec un disque SSD puis HDD.
   http://www.01net.com/actualites/failles-cpu-jusqu-a-21-percent-de-baisse-de-performance-sur-les-processeurs-intel-recents-1348158.html

3. **Skype adopte le chiffrement de bout en bout**

   Mieux vaut tard que jamais. Microsoft vient d'annoncer une nouvelle fonction dans Skype qui permettra aux utilisateurs d'avoir des conversations écrites ou vocales chiffrées de bout en bout. Baptisée « Private Conversations », cette option n'est disponible pour l'instant que dans la version bêta (Insider Preview). Evidemment, elle ne fonctionnera que si l'interlocuteur dispose également de cette version. Par ailleurs, elle ne s'applique pas aux discussions de groupe, ni aux chats vidéo.
   http://www.01net.com/actualites/skype-adopte-enfin-le-chiffrement-de-bout-en-bout-1347876.html

4. **7 questions pour comprendre les méga failles des processeurs**

   PC de bureau, PC portables, smartphones, serveurs… Un grand nombre de systèmes informatiques sont vulnérables aux attaques Meltdown et Spectre qui exploitent des faiblesses dans les processeurs. Voici les points essentiels pour tout comprendre.
   http://www.01net.com/actualites/intel-amd-arm-7-questions-pour-comprendre-les-mega-failles-des-processeurs-1341798.html

5. **Un pirate pédophile a espionné des PC pendant 13 ans**

   Depuis un an, les chercheurs en sécurité tentent de percer le secret de FruitFly, un mystérieux logiciel d'espionnage qui infecte des ordinateurs Mac. En janvier 2017, la société MalwareBytes est la première à analyser ce malware trouvé sur des ordinateurs d'instituts de recherches biomédicales. Le code est assez bizarre. Il est à la fois sophistiqué et démodé, certaines fonctions et librairies remontant en effet aux années 90, ce qui n'empêche pas de fonctionner parfaitement.
   http://www.01net.com/actualites/un-pirate-pedophile-a-espionne-des-milliers-d-utilisateurs-de-pc-pendant-13-ans-1347417.html

6. **Des failles permettent d'espionner les discussions de groupe sur WhatsApp**
   En adoptant par défaut le chiffrement de bout en bout en 2016, la messagerie instantanée WhatsApp a fait une énorme contribution pour la protection des données personnelles de ses utilisateurs. Toutefois, l'implémentation technique relative aux discussions de groupe n'est pas parfaite, comme viennent de le constater des chercheurs en sécurité de l'université allemande Ruhr-University Bochum. L'objectif du chiffrement de bout en bout est d'éliminer le risque provenant des serveurs de relais intermédiaires, qui pourraient être infectés par des pirates ou réquisitionnés sur demande gouvernementale.
   http://www.01net.com/actualites/whatsapp-des-failles-permettent-d-espionner-les-discussions-de-groupe-1347179.html

7. **Bientôt un wifi plus sécurisé grâce au WPA3**
   Le consortium Wi-Fi Alliance a profité du CES 2018 pour annoncer la disponibilité prochaine d'une nouveau standard cryptographique censé améliorer la confidentialité des échanges sur les réseaux sans fil. Il faut dire que l'année 2017 n'a pas été triste de ce point de vue. En octobre dernier, le chercheur en sécurité Mathy Vanhoef avait dévoilé l'attaque Krack qui permettait de casser le chiffrement WPA2 pour tous les terminaux sans fil. Des patchs ont certes été diffusés, mais encore faut-il qu'ils soit déployés et installés, ce qui est loin d'être simple au niveau des smartphones Android ou des objets connectés.
   http://www.01net.com/actualites/ces-2018-bientot-un-wi-fi-beaucoup-plus-securise-grace-au-wpa3-1345588.html

8. **Avec Encrypted Traffic Analytics, Cisco détecte les malware dans le trafic chiffré**

   Cisco commercialise sa solution Encrypted Traffic Analytics (ETA). Ce système de surveillance des métadonnées de paquets réseau peut maintenant détecter le trafic malveillant même s'il est chiffré.
   https://www.lemondeinformatique.fr/actualites/lire-avec-encrypted-traffic-analytics-cisco-detecte-les-malware-dans-le-trafic-chiffe-70511.html

IV. NOTES IMPORTANTES

1. Veuillez enregistrer l'adresse alerts@antic.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. 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.

3. 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

4. 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 l'adresse email alerts@antic.cm ou au numéro de téléphone **242 09 91 64**.