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 Mai 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	Une vulnérabilité a été corrigée dans Google Chrome. L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant d'accéder aux informations confidentielles. Les versions affectées sont celles antérieures à 66.0.3359.170 pour Windows, Mac et Linux	11/05/2018	CVE-2018-6122	66.0.3359.170 Télécharger	Mettre à jour le navigateur	7.4
Vulnérabilités dans Mozilla Firefox	Plusieurs vulnérabilités ont été corrigées dans Mozilla Firefox. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Firefox versions antérieures à 60	10/05/2018	CVE-2018-5183	60.0 Télécharger	Mettre à jour le navigateur	9.4
Vulnérabilités dans Microsoft IE et EDGE	Plusieurs vulnérabilités ont été corrigées dans Microsoft IE et Edge. Elles permettent à un attaquant de provoquer une divulgation d'informations, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	09/05/2018	CVE-2018-8178	IE 11	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 dans Microsoft Windows. Elles permettent à un attaquant de provoquer une divulgation d'informations, une élévation de privilèges, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	09/05/2018	CVE-2017-8174	Windows 10	Effectuer une mise à jour via Windows Update	10.0
Vulnérabilité dans certains produits Microsoft	Plusieurs vulnérabilités ont été corrigées dans certains produits Microsoft. Elles permettent à un attaquant de provoquer une divulgation d'informations, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité. Les systèmes infectés sont les suivants : • C SDK pour Azure IoT • C# SDK pour Azure IoT • ChakraCore • Java SDK pour Azure IoT • Microsoft Infopath 2013 Service Pack 1 (édition 32 et 64 bits)	09/05/2018	CVE-2017-8178	Windows 10	Effectuer une mise à jour via Windows Update	10.0

Vulnérabilité dans Google Chrome OS	Google annonce des vulnérabilités non spécifiées sur Chrome OS versions antérieures à 66.0.3359.158 (Platform version: 10452.85.0)	09/05/2018	–	66.0.3359.170 Télécharger	Effectuez une mise à jour du système	9.0
Vulnérabilité dans le Noyau Linux de RedHat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de RedHat. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.	09/05/2018	CVE-2017- 1000199	4.17-rc5 Télécharger	Effectuez une mise à jour du système	10.0
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 élévation de privilèges. Les versions infectées sont les suivantes : • Ubuntu 17.10 • Ubuntu 16.04 LTS • Ubuntu 14.04 LTS • Ubuntu 12.04 ESM	09/05/2018	CVE-2017- 1000199	4.17-rc5 Télécharger	Effectuez une mise à jour du système	7.1

Vulnérabilité dans le Noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Certaines d'entre 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 : • SUSE OpenStack Cloud 6 • SUSE Linux Enterprise Server for SAP 12-SP1 • SUSE Linux Enterprise Server 12-SP1-LTSS • SUSE Linux Enterprise Module for Public Cloud 12 • SUSE Linux Enterprise Server 12-LTSS • SUSE Linux Enterprise Real Time Extension 12-SP3 • SUSE Linux Enterprise Server for SAP 12-SP2	14/05/2018	CVE-2017- 1000199	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 Cisco WebEx Network Recording Player	Une vulnérabilité a été corrigée dans Cisco WebEx Network Recording Player pour Advanced Recording Format (ARF). Un attaquant distant pourrait exploiter cette vulnérabilité en envoyant à un utilisateur un fichier malicieux au format ARF via email ou via une URL pour exécuter du code arbitraire à distance. Les systèmes infectés sont les suivants : • Cisco WebEx Meeting Server builds antérieure à 3.0 Patch 1 • Cisco WebEx Meetings with client builds antérieure à T32.12 • Cisco WebEx Business Suite (WBS31) client builds antérieure à T31.23.4	08/05/2018	CVE-2018-0264	-	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-war	5.3

Vulnérabilité dans 7-Zip	Une vulnérabilité a été corrigée dans 7-Zip. L'exploitation de cette vulnérabilité peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes infectés sont les suivants : 7-Zip versions antérieures à 18.05 SINAMICS GM150 V4.7 avec PROFINET versions antérieures à V4.8 SP2	09/05/2018	CVE-2018-10115	18.05 Télécharger	Effectuez une mise à jour	10.0
Vulnérabilité dans Citrix XenServer	Plusieurs vulnérabilités ont été corrigées dans Citrix XenServer. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à l'intégrité des données.	10/05/2018	CVE-2018-8897	7.4 Télécharger	Effectuez une mise à jour du système	6.0
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.	09/05/2018	CVE-2018-8168	-	Correctif disponible via Windows Upadte	7.3
Vulnérabilité dans Microsoft Exchange Server	Plusieurs vulnérabilités ont été corrigées dans Microsoft Exchange Server. Elles permettent à un attaquant de provoquer une divulgation d'informations, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	09/05/2018	CVE-2018-8178	–	Correctif disponible via Windows Upadte	9.1

Critique faille affectant S/MIME et PGP	Une faille, nommée efail présente dans plusieurs implémentations des standards OpenPGP et S/MIME au sein de différents clients de messagerie a été récemment découverte par des chercheurs. L'exploitation de cette vulnérabilité permet dans certaines conditions à un attaquant de déchiffrer un email pourtant protégé par PGP ou S/MIME. La réussite de cette attaque nécessite qu'un attaquant soit en mesure de récupérer la copie d'un mail chiffré. Une fois en possession de celui-ci, il peut créer une version modifiée de cet email, dont le contenu chiffré est compris dans une balise HTML contenant un lien vers un domaine contrôlé par l'attaquant. L'attaquant doit ensuite renvoyer ce mail piégé vers la cible : en l'ouvrant, celui-ci déchiffrera le message et une copie en clair sera envoyée vers le nom de domaine contenu dans la balise HTML, permettant à l'attaquant de le récupérer. Pour plus d'informations sur l'exploitation de la faille efail, veuillez-vous référer à l'article détaillant la vulnérabilité sur le lien suivant : https://efail.de/efail-attack-paper.pdf Les chercheurs estiment donc que la correction de cette vulnérabilité devra se faire au sein des spécifications d'OpenPGP et S/MIME afin de parvenir à un résultat uniforme dans toutes les implémentations de ces algorithmes. Solutions : En attendant la publication des correctifs, il est recommandé d'appliquer temporairement les mesures ci-après : • Désactiver l'utilisation du contenu HTML dans le client de messagerie ; • Déchiffrer le courrier en dehors du client de messagerie ; • Désactiver le chargement du contenu à distance par le client de messagerie. Références : • Site détaillant le principe de la vulnérabilité du 14 mai 2018 https://efail.de/ • Article de recherche présentant les travaux sur la vulnérabilité EFAIL https://efail.de/efail-attack-paper.pdf • Désactivation du contenu HTML dans Thunderbird http://kb.mozillazine.org/Plain_text_e-mail_(Thunderbird)#Displaying_messages • Désactivation du contenu HTML dans Outlook https://support.microsoft.com/en-us/help/831607/how-to-view-all-e-mail-messages-inplain-text-format

III. ACTUALITÉS

1. Failles critiques dans adobe pdf….

Si vous utilisez une Adobe Acrobat ou Reader pour lire vos PDF, mettez immédiatement à jour vos logiciels. L'éditeur vient de publier en urgence une rafale de patchs pour combler 47 failles, dont 24 considérées comme critiques. Ces vulnérabilités affectent les logiciels Acrobat DC, Acrobat Reader DC, Acrobat 2017 et Acrobat Reader DC 2017, aussi bien sur Windows que macOS. Inutile de dire que cette mise à jour est classée au plus haut niveau de priorité. http://www.01net.com/actualites/failles-critiques-pdf-adobe-publie-une-rafale-de-patchs-en-urgence-1446630.html

2. Facebook suspend 200 applications suspectées de détournées les données personnelles

Chose promise, chose due. L'enquête lancée par Mark Zuckerberg a révélé l'existence de 200 applications tierces suspectées de détourner les données personnelles de leurs utilisateurs, à leur insu. Une pratique qui a été pointée du doigt lors de l'affaire de Cambridge Analytica : un utilisateur Facebook utilise une appli des plus banales, comme un quizz, et autorise l'exploitation de ses données ainsi que celles de ses amis à un sous-traitant, sans le savoir.
http://www.01net.com/actualites/facebook-suspend-200-applications-suspectees-de-detourner-nos-donnees-personnelles-1445665.html

3. Des failles critiques permettant de lire des mails chiffrés

Au niveau du grand public, la technologie la plus connue des deux est OpenPGP que l'on peut utiliser avec n'importe quel client de messagerie. Il suffit d'installer le plugin logiciel ou l'extension de navigateur approprié : Enigmail, GPGTools, Gpgf4win, Mailvelope, etc. Certains fournisseurs de services l'ont également intégré directement dans leurs offres. C'est le cas par exemple de ProtonMail et de GMX Caramail. La techno S/MIME, quant à elle, est utilisée uniquement en entreprise, car elle nécessite une infrastructure hiérarchique pour distribuer des certificats aux utilisateurs.

http://www.01net.com/actualites/des-failles-permettent-de-lire-les-mails-chiffres-par-openpgp-ou-smime-1445195.html

4. Chassées du Playstore ces malwares sont de retour

La boutique applicative de Google continue d'être gangrenée par les fausses applis. Des chercheurs en sécurité viennent récemment de détecter des dizaines d'applis Android qui, sous couvert d'une fonctionnalité banale, procède à des activités malveillantes comme l'affichage de publicités ou la redirection vers des sites d'arnaques.

http://www.01net.com/actualites/chasses-du-play-store-ces-malwares-sont-de-retour-apres-un-changement-de-nom-1444893.html

5. Stockage cloud quelles alternatives pour quels prix ?

Alors que les nouveaux forfaits de stockage de Google viennent d'être dévoilés, nous avons décidé de faire un tour d'horizon des principales offres équivalentes chez ses concurrents. L'espace de stockage n'est désormais plus le seul argument, les services sont maintenant partie prenante des offres. Assistance, effacement à distance, suite bureautique ou gestion de comptes bancaires sont en effet intégrés à certains services. Tous les prix ici le sont à titre mensuel

.http://www.01net.com/actualites/stockage-cloud-quelles-alternatives-a-google-one-et-pour-quel-prix-1445823.html

6. Les applications Linux débarquent sur les Chromebook

Lors de la conférence Google I/O 2018, Google a fait une annonce qui fera plaisir à tous les utilisateurs d'applications Linux. En effet, les prochaines versions de Chrome OS disposeront d'une machine virtuelle pour les exécuter, connue auparavant sous le nom de projet Crostini

http://www.01net.com/actualites/les-applications-linux-debarquent-sur-les-chromebook-1441452.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**.