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 Février 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 Mozilla Firefox	Une vulnérabilité a été corrigée dans Firefox. L'exploitation de cette vulnérabilité peut permettre à un attaquant de prendre le contrôle d'un système affecté.	30/01/2018	CVE-2018-5124	58.0.1 Télécharger	Mettre à jour le navigateur	9.0
Vulnérabilité dans Google Chrome	Plusieurs vulnérabilités ont été corrigées dans Google Chrome et Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	04/02/2018	CVE-2018-6054	64.0.3282.140 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Google Android	Plusieurs vulnérabilités ont été corrigées dans Google Android. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service et une atteinte à la confidentialité des données.	06/02/2018	CVE-2007-17770	8 (Oreo) https://www.android.com/	Effectuez une mise à jour du système	10.0

II.2 Systèmes d' exploitation

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 et une élévation de privilèges. Les systèmes affectés sont les suivants : - SUSE Linux Enterprise Server 12-LTSS - SUSE Linux Enterprise Server 12-SP1-LTSS - SUSE Linux Enterprise Server for SAP 12-SP1 - SUSE Linux Enterprise Live Patching 12	29/01/2018	CVE-2017-17712	42.3 Télécharger	Appliquer le patch de sécurité disponible à l'adresse : https://www.suse.com/support/update/announcement/2018/suse-su-20180294-1/	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 l'exécution de code arbitraire, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : - Ubuntu 16.04 LTS - Ubuntu 17.10	29/01/2018	CVE-2017-5753	16.04.03 LTS Télécharger	Veuillez-vous référer au guide de sécurité de linux Ubuntu pour obtenir les correctifs. https://usn.ubuntu.com/usn/usn-3548-1//	10.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Flash Player 28.0.0.137	Une vulnérabilité critique de type Zero-Day existe dans Adobe Flash Player 28.0.0.137 et les versions antérieures. Une exploitation réussie pourrait potentiellement permettre à un attaquant de prendre le contrôle du système affecté. Adobe annonce qu'un exploit pour cette vulnérabilité portant l'identifiant CVE-2018-4878 existe et qu'il est utilisé dans des attaques ciblées contre des utilisateurs Windows. Ces attaques exploitent les documents Office avec du contenu Flash malveillant intégré distribué par courrier électronique. **Solution** : Adobe annonce que des correctifs sont prévus pour la semaine du 5 février 2018. Dans l'attente de la publication de ces correctifs, le CIRT recommande : - De s'assurer que le mode protégé d'Office est bien activé car il empêche l'exécution automatique du Flash Player pour les documents téléchargés sur internet. Pour plus d'information sur l'activation du Mode Protégé d'office veuillez cliquer ici - De désactiver les greffons Flash Player ; - De toujours se méfier de tout document non sollicité envoyé par courrier électronique et de ne jamais cliquer sur les liens à l'intérieur de ces documents, sauf en cas de vérification de la source **Risque :** - Exécution du code arbitraire à distance. - Perte de contrôle du système affecté.					

Vulnérabilité Lenovo	**Système affecté :** Les ordinateurs portables ThinkPad X1 Carbon 5ème génération fabriqués entre Décembre 2016 et Octobre 2017, avec un code «Machine Type» de 20HQ, 20HR, 20K3 ou 20K4. La société Lenovo a annoncé le 07/02/2018 que les ordinateurs portables ThinkPad X1 Carbon 5ème génération fabriqués entre Décembre 2016 et Octobre 2017 sont concernés par un défaut de fabrication qui pourrait endommager la batterie et provoquer une surchauffe, ce qui pourrait poser un risque d'incendie. Plus de 83 500 ordinateurs portables touchés, probablement plus. Lenovo a déclaré que seuls les ordinateurs portables ThinkPad X1 Carbon avec un code «Machine Type» de 20HQ, 20HR, 20K3 ou 20K4 sont concernés. Les propriétaires de ces machines peuvent trouver ce code sur un autocollant à l'arrière de l'ordinateur portable. **Solution :** Lenovo a créé une page Web dans laquelle les utilisateurs peuvent saisir leur numéro de série et savoir s'ils doivent contacter un représentant Lenovo pour faire remplacer leur appareil. Pour plus d'informations Veuillez consulter la page **Risque :** Risque d'incendie					
Vulnérabilité dans Gemalto Sentinel	Plusieurs vulnérabilités ont été corrigées dans Gemalto Sentinel License Manager. L'exploitation réussie de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire à distance ou de provoquer un déni de service, rendant le service Sentinel LDK License Manager indisponible. Le système affecté est le suivant : - Gemalto Sentinel License Manager version antérieure à 7.6	02/02/2018	CVE-2017-11498	Contacter Gemalto	Veuillez-vous référer au guide de sécurité de pour obtenir les correctifs https://sentinelcustomer.gemalto.com/sentineldownloads/	6.2

Vulnérabilité dans les produits VMWARE	Plusieurs vulnérabilités ont été corrigées dans les produits VMware vRealize Automation, vSphere Integrated Containers et AirWatch Console. Un attaquant pourrait exploiter ces vulnérabilités pour prendre le contrôle d'un système affecté.	29/01/2018	CVE-2017-4159	En savoir plus	Appliquer les patchs de sécurité	10.0
Vulnérabilité dans les produits CISCO	Cisco a publié une mise à jour de sécurité pour corriger une vulnérabilité qui affecte le système Adaptive Security Appliance (ASA) et le système Firepower. L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant de prendre le contrôle d'un système affecté.	30/01/2018	CVE-2018-0101	Contacter Cisco	Veuillez-vous référer au guide de sécurité de CISCO pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1	7.8

Vulnérabilité dans PHP	Plusieurs vulnérabilités ont été corrigées dans PHP. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et un déni de service. Les systèmes affectés sont les suivants : - PHP versions 7.1.x antérieures à 7.1.14 - PHP versions 7.2.x antérieures à 7.2.2	06/02/2018	-	7.2.2 Téléchargez	Veuillez-vous référer au guide de sécurité de PHP pour obtenir les correctifs. http://www.php.net/ChangeLog-7.php#7.1.14 http://www.php.net/ChangeLog-7.php#7.2.2	7.2
Vulnérabilité dans Juniper Junos OS	Une vulnérabilité a été corrigée dans Juniper Junos OS. Elle permet à un attaquant de provoquer un déni de service à distance.	06/02/2018	CVE-2018-0002	Contacter Juniper	Veuillez-vous référer au guide de sécurité de Juniper JSA10829 pour obtenir les correctifs. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10829&cat=SIRT_1&actp=LIST	6.3

III. ACTUALITÉS

1. **Windows defender fait désormais la chasse aux scarewares**
   Microsoft vient de mettre à jour la liste de logiciels susceptibles d'être supprimés par Windows Defender pour inclure les « scarewares ». Ces programmes pseudo-utilitaires incitent les utilisateurs à payer pour un service souvent inutile en les effrayant avec des messages sur la sécurité ou la performance : *« Attention, votre ordinateur est infecté ! »*, *« Alerte virus »*, *« Vous avez 2695 erreurs dans votre système »*, etc. Souvent, les scarewares proposent un scan gratuit dont le résultat est évidemment désastreux. Pour résoudre le problème, l'utilisateur est prié de mettre la main à la poche.
   http://www.01net.com/actualites/windows-defender-fait-desormais-la-chasse-aux-scarewares-1363756.html

2. **Un correctif Microsoft afin de contrer celui d'Intel**
   Les correctifs contre les attaques Spectre et Meltdown se suivent mais ce n'est hélas pas pour aider l'utilisateur. Microsoft vient de publier en urgence la mise à jour KB4078130 pour annuler les effets du patch d'Intel contre la variante 2 de l'attaque Spectre. En effet, ce correctif pose des problèmes de redémarrages intempestifs : Intel a même recommandé à ses partenaires d'arrêter son déploiement. Le patch de Microsoft est donc conçu pour arrêter la casse en attendant qu'Intel propose une nouvelle version de son correctif, sans les effets secondaires néfastes.
   http://www.01net.com/actualites/failles-cpu-microsoft-publie-un-correctif-d-urgence-pour-windows-afin-de-contrer-celui-d-intel-1360822.html

3. **De mystérieux prototypes de malware circulent sur la toile**
   A ce jour, aucune victime n'est à déplorer, mais de mystérieux prototypes de malware Meltdown/Spectre circulent désormais sur la Toile, comme l'explique Fortinet dans une note de blog. Ainsi, 119 programmes uniques exploitant les failles Meltdown ou Spectre sont apparus entre le 7 et le 22 janvier. Cette analyse s'appuie sur la base de données du laboratoire antiviral AV-Test. Contacté par 01net.com, AV-Test nous révèle que le compteur atteint désormais 139 fichiers uniques.
   http://www.01net.com/actualites/failles-cpu-de-mysterieux-prototypes-de-malware-circulent-sur-la-toile-1363055.html

4. **Plus de 700.000 applications malicieuses retirées de Google Play en 2017**

   Google ne lâche rien dans sa chasse aux applications véreuses : dans un post sur le blog des développeurs d'Android, le responsable de Google Play Andrew Ahn a affirmé que Google avait retiré plus de 700.000 apps en 2017. Un chiffre en augmentation de 70% par rapport à 2016. Selon Andrew Anh, « *99% des applications avec du contenu interdit ont été identifiées et rejetées avant que quiconque n'ait pu les installer* ». De quoi redorer un peu le blason de Google Play qui fait un peu far west à côté de l'App Store d'Apple où chaque envoi et mise à jour doit être validée avant publication.
   http://www.01net.com/actualites/plus-de-700-000-applications-malicieuses-retirees-de-google-play-en-2017-1362542.html

5. **Intel donne aux robots et aux PC la capacité de voir comme un humain**
   Le géant de Santa Clara vient de lancer deux nouvelles caméras 3D abordables qui peuvent être utilisées facilement et offrent une « vision humaine » à nos drones, robots et ordinateurs.
   http://www.01net.com/actualites/intel-donne-a-n-importe-quel-pc-ou-robot-la-capacite-de-voir-comme-un-humain-1353560.html

6. **Les apps de sport révèlent des secrets des bases américaines**
   Les services armés du monde entier doivent en avoir marre des réseaux sociaux ! En cible cette fois-ci, le service Strava, une application de sport qui permet non seulement de mesurer ses performances mais qui sert aussi de réseau social pour sportifs. Le problème pour l'armée américaine comme le relève The Verge, c'est que Strava a dévoilé une « heatmap », ou carte de chaleur de ses utilisateurs, qui répertorie des milliards d'activités et qui a permis à un analyste en sécurité de montrer qu'elle permettait de dévoiler des détails… des bases américaines.
   http://www.01net.com/actualites/les-apps-de-sport-revelent-des-secrets-des-bases-americaines-1360763.html

7. **Chiffrement des données Android comment ça marche ?**
   Qu'il s'applique à un ordinateur ou à un téléphone, la logique du chiffrement demeure inchangée. Il s'agit de rendre le contenu illisible en « mélangeant » les 0 et les 1 qui constituent tout fichier numérique. Une clé unique est générée, plus ou moins complexe selon les cas, et permet de restaurer les données. Android utilise l'algorithme de chiffrement AES 128-Bit. Depuis Lollipop (Android 5.0), la clé principale, c'est-à-dire celle qui déverrouille les données, est conservée dans un environnement sécurisé appelé Trusted Execution Environment (ou environnement d'exécution de confiance).
   http://www.01net.com/actualites/chiffrement-des-donnees-android-comment-ca-marche-1357281.html

8. **Les pirates de Dark caracal espionnent des smartphones Android dans le monde entier**
   Des centaines de gigaoctets de données volées auprès de milliers de personnes dans plus de vingt pays, et cela en ciblant principalement des smartphones Android. Bienvenue dans l'antre de « Dark Caracal », un groupe de pirates de haut vol dont l'existence vient d'être révélée par les chercheurs en sécurité de l'éditeur Lookout et de l'association Electronic Frontier Foundation (EFF). Selon eux, il s'agirait même de la première campagne d'espionnage mobile réellement globale découverte à ce jour.
   http://www.01net.com/actualites/les-pirates-de-dark-caracal-espionnent-des-smartphones-android-dans-le-monde-entier-1355559.html

9. **Cisco comble une vulnérabilité importante de ses firewalls**
   Si Spectre et Meltdown ne lui avaient pas volé la vedette, la nouvelle faille de Cisco aurait pu faire un bon candidat pour la faille du début d'année. Celle-ci ne dispose pas de petit nom, encore moins de logo dédié, mais elle a le mérite de décrocher un score de 10/10 sur l'échelle de sévérité des failles (CVSSv3). Cette faille affecte de nombreux produits Cisco embarquant la suite logicielle Adaptive Security Appliance et ayant recours à la fonctionnalité SSL VPN. Comme l'explique Cisco, un attaquant pourrait exploiter cette faille afin faire crasher la machine vulnérable, ou bien de la pousser à exécuter du code inconnu et potentiellement malveillant, le tout à distance.
   http://www.zdnet.fr/actualites/cisco-comble-une-vulnerabilite-importante-de-ses-firewalls-39863542.htm

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**.