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 2019

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	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes n'intégrant pas le correctif de sécurité du 7 janvier 2019, sont affectés	07/01/2019	CVE-2017-18281	70.0.3578.98 Télécharger	Effectuez une mise à jour du navigateur	10.0
Vulnérabilité dans IE et Edge	De multiples vulnérabilités ont été corrigées dans Microsoft Edge et IE. Elles permettent à un attaquant de provoquer une élévation de privilèges et une exécution de code à distance.	09/01/2019	CVE-2018-0568	-	Mettre à jour le système via Windows Update	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, une exécution de code à distance et une usurpation d'identité.	09/01/2019	CVE-2018-0588	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et une exécution de code à distance.	09/01/2019	CVE-2018-0584	_	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Fortinet FortiOS	De multiples vulnérabilités ont été découvertes dans Fortinet FortiOS et FortiClient. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un déni de service. FortiOS versions 5.6.0 et antérieures	11/01/2019	CVE-2018-1352	5.6.0 Contacter	Effectuez une mise à jour	4.3

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	De multiples vulnérabilités ont été corrigées dans Microsoft .Net. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un déni de service. Les versions affectées sont les suivants : Microsoft .NET Framework 4.7.2	09/01/2019	CVE-2018-0564	4.7.2	Effectuez une mise à jour du système Windows Update	4.4
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, une exécution de code à distance et une usurpation d'identité.	09/01/2019	CVE-2018-0585		Veuillez-vous référer au guide de sécurité https://portal.msrc.microsoft.com/fr-FR/security-guidance	4.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Acrobat et Reader	De multiples vulnérabilités ont été découvertes dans Adobe Acrobat et Reader. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges. Les systèmes affectés sont les suivants : Acrobat Reader DC versions antérieures à 2019.010.20069 sur Windows et macOS	04/01/2019	CVE-2018-19717	2019.010.20069 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/acrobat/apsb19-02.html	7.8
Vulnérabilité dans les produits IBM	De multiples vulnérabilités ont été découvertes dans les produits IBM. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données. les systèmes infectés sont les suivants : IBM Security Identity Manager versions 7.0.1 à 7.0.1.10 IBM Spectrum Control versions 5.2.8 à 5.2.13 IBM Tivoli Storage Productivity Center versions 5.2.0 à 5.2.7.1	14/01/2019	CVE-2018-1969	Contacter IBM	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www-01.ibm.com/support/docview.wss?uid=ibm10793725	2.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 et un déni de service à distance. Les versions affectées sont les suivantes : PHP versions 7.x antérieures à 7.3.1 **NB :** Le support de PHP 5 est terminé.	11/01/2019	CVE-2018-19935	7.3.1 Télécharger	Effectuez une mise à jour	5.1
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service. Wireshark versions 2.6.0 à 2.6.5	08/01/2019	CVE-2019-5719	2.9.0 Télécharger	Effectuez une mise à jour	6.2

III. ACTUALITÉS

1. Des vulnérabilités zéro day découvertes dans les technologies d'accès aux bâtiments

La société de « Cyber Exposure » Tenable, annonce avoir découvert plusieurs vulnérabilités du système de contrôle d'accès PremiSys™ développé par IDenticard. Lorsqu'elle est exploitée, la vulnérabilité la plus grave donne à l'attaquant un libre accès à la base de données du système de badges, ce qui lui permet d'entrer clandestinement dans les bâtiments en créant des badges frauduleux et en désactivant les serrures des bâtiments. D'après les informations disponibles sur son site Web, IDenticard compte des dizaines de milliers de clients dans le monde entier, y compris des entreprises Fortune 500, des écoles primaires et secondaires, des universités, des centres médicaux et des agences gouvernementales

https://www.datasecuritybreach.fr/de-multiples-vulnerabilites-zero-day-decouvertes-dans-les-technologies-dacces-aux-batiments/

2. Prison pour un vendeur de DDoS

Daniel Kaye, 30 ans, qui se faisait appeler dans l'underground « BestBuy » et « Popopret » vient d'écoper de deux ans et huit mois de prison ferme pour avoir lancé des attaques de type DDoS. Des Dénis Distribués de Service qui ont visé, entre autres, Lonestar Cell MTN, une société de télécommunication basée au Libéria.

https://www.datasecuritybreach.fr/prison-pour-un-vendeur-de-ddos/

3. Des vulnérabilités system down pour les distributions linux

Le laboratoire de la société Qualys vient de révéler trois vulnérabilités exploitables localement dans systemd-journald, un composant central présent dans toutes les distributions Linux. Ces vulnérabilités sont baptisées « System Down » en référence au groupe de Rock, System of a Down. L'avis de sécurité complet est ici. CVE-2018-16864 et CVE-2018-16865, deux corruptions de mémoire (alloca () s) contrôlé par l'attaquant;

https://www.datasecuritybreach.fr/system-down-pour-les-distributions-linux/

4. Des failles et bugs corrigés dans symphony

Le framework Symfony est un environnement informatique qui a fait ses preuves. Un bel outil robuste, proposant des fonctionnalités de cybersécurité. Authentification, gestion des sessions, … Symfony permet d'assurer la sécurité à la condition d'être prise au sérieuse. C'est d'ailleurs pour cela qu'une mise à jour, la 3.4.20, a été diffusée, début décembre 2018. 12 bugs et 2 problèmes sérieux de sécurité ont été corrigés. [CVE-2018-19790]

https://www.datasecuritybreach.fr/failles-et-bugs-corriges-dans-symfony-3-4-20/

5. Deux nouveaux malwares Servhelper et Flawedgrace

Utilisés par TA505, ServHelper est un malware précédemment non documenté, distribué en deux variantes : l'une axée sur les fonctions de bureau à distance et l'autre qui fonctionne principalement comme un « downloaders ». Quant à FlawedGrace, c'est un RAT également non documenté auparavant, qui est apparu dans un certain nombre de campagnes ServHelper TA505. TA505 semble cibler activement les banques, le retail et les restaurants. Ce ciblage est conforme aux autres activités que nous avons signalées plus tôt en 2018 sur le blog Proofpoint.

https://www.undernews.fr/malwares-virus-antivirus/servhelper-et-flawedgrace-2-nouveaux-malwares-introduits-par-ta505.html

6. Ryuk le ransomware taillé pour la pêche aux gros

Un nouveau rançongiciel terrorise depuis moins d'un an les entreprises, en particulier américaines. Baptisé « Ryuk », il s'agit d'un malware que les pirates utilisent pour attaquer de manière chirurgicale les ressources stratégiques dans un réseau. Ce qui permet de maximiser la rançon. La campagne a été analysée concomitamment par les chercheurs de Crowdstrike et FireEye, qui ont estimé que les pirates ont d'ores et déjà pu récolter depuis février 2017 l'équivalent de 3,2 millions d'euros au travers de 52 transactions, soit une rançon moyenne d'environ 60.000 euros par victime.

https://www.01net.com/actualites/ryuk-le-ransomware-taille-pour-la-peche-au-gros-recolte-des-millions-d-euros-1611144.html

7. Pirater un Iphone et devenez millionnaire

Le marché des failles de sécurité est en pleine forme. Zerodium, le broker le plus connu en la matière, vient de publier une nouvelle liste de prix d'achat. Un jailbreak d'iOS réalisé à distance et sans intervention de l'utilisateur (« zero click ») passe de 1,5 à 2 millions de dollars. Un piratage similaire avec intervention de l'utilisateur (« one click ») augmente aussi passant de 1 à 1,5 million de dollars.

https://www.01net.com/actualites/si-vous-arrivez-a-pirater-l-iphone-vous-pouvez-devenir-multimillionnaire-1606514.html

8. Un jeune pirate de 20 ans auteur d'un vol de données en Allemagne

L'affaire avait fait grand bruit vendredi dernier. Les données personnelles d'un millier de personnalités allemandes, dont des centaines de politiciens, avaient été publiées sur le Web : noms, adresses, e-mails, messages instantanés, photos, etc. Contrairement à ce que l'on pouvait croire, cette fuite ne serait pas l'œuvre d'un groupe de hackers ou d'une organisation étatique, mais d'une personne isolée.

https://www.01net.com/actualites/un-jeune-de-20-ans-serait-l-auteur-de-l-incroyable-vol-de-donnees-personnelles-en-allemagne-1606329.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**.