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 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	Google a publié la version de Chrome 72.0.3626.81 pour Windows, Mac et Linux. Cette version corrige plusieurs vulnérabilités qu'un attaquant pourrait exploiter pour prendre le contrôle d'un système affecté. Les systèmes infectés sont les suivants : Google Chrome versions antérieures à 72.0.3626.81sur Windows, Mac et Linux	30/01/2019	CVE-2017-17481	72.0.3626.81 Télécharger	Effectuez une mise à jour du navigateur	10.0
Vulnérabilité dans Mozilla Firefox ESR	Plusieurs vulnérabilités ont été corrigées dans Mozilla Firefox. Un attaquant pourrait exploiter ces vulnérabilités pour prendre le contrôle d'un système affecté. Les versions concernées sont les suivantes : Mozilla Firefox ESR de versions antérieures à la version 60.5	30/01/2019	CVE-2018-18498	60.5 Télécharger	Mettre à jour le navigateur	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. 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 systèmes infectés sont les suivants : Ubuntu 18.04 LTS	29/01/2019	CVE-2018-14625 CVE-2018-16882 CVE-2018-19407 CVE-2018-19854	18.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3872-1/	10.0
Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Google Chrome OS toutes versions antérieures à 71.0.3578.127 (Platform version: 11151.113.0)	17/01/2019		71.0.3578.127 Contacter	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-chrome-os.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29	9.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	De multiples vulnérabilités ont été découvertes dans Drupal. 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 : Drupal versions 8.6.x antérieures à 8.6.6.	17/01/2019	CVE-2018-1000888	8.6.6 Télécharger	Mettre à jour le CMS	10.0
Vulnérabilité dans le CMS Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : Moodle versions 3.6.x antérieures à 3.6.2	21/01/2019	CVE-2019-3810	3.6.2 Télécharger	Mettre à jour le CMS	10.0
Vulnérabilité dans le CMS Joomla	Joomla annonce la disponibilité d'une mise à jour traitant plusieurs vulnérabilités pour son CMS Joomla. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'injection de code indirecte à distance. Les versions affectées sont celles antérieures à 3.9.2 et postérieure à 2.5.0	17/01/2019	CVE-2019-6264	3.9.2 Télécharger	Mettre à jour le CMS	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Exchange Server (zero-day)	**Bilan de la vulnérabilité :** Une faille critique a été découverte dans le Serveur Microsoft Exchange. L'exploitation de cette faille peut permette à un utilisateur malveillant disposant d'un compte exchange de réussir une élévation de privilèges et obtenir le droit Admin sur le Contrôleur de Domaine. **Solution :** Microsoft annonce qu'une mise à jour sera programmée dans le mois Février 2019. Dans l'attente de la publication du correctif, il est recommandé de : Réduire les privilèges Exchange; - Activer la signature LDAP et channel binding ; - Empêcher les serveurs Exchange de se connecter à des ports arbitraires; - Supprimer la clé de registre qui permet le relais; - Activer la signature SMB.					
Vulnérabilité dans Adobe Experience Manager	Adobe a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités dans Adobe Experience Manager. Un attaquant pourrait exploiter ces vulnérabilités pour obtenir des informations sensibles. Les systèmes affectés sont les suivants : Adobe Experience Manager 6.4,	23/01/2019	CVE-2018-19726	6.4 Contacter	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/aem-forms/apsb19-03.html	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Apple	De multiples vulnérabilités ont été découvertes dans les produits Apple. 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 l'intégrité des données. iOS versions antérieures à 12.1.3	23/01/2019	CVE-2019- 6235	12.1.3 Site web	Effectuez une mise à jour du système	5.6
Vulnérabilité dans Nagios	Une vulnérabilité a été découverte dans Nagios. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Nagios versions antérieures à 4.4.3.	16/01/2019	CVE-2018-19935	4.4.3 Télécharger	Effectuez une mise à jour	5.1
Vulnérabilité dans les produits CISCO	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Certaines d'entre elles permettent 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.	16/01/2019	CVE-2019-1651	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-bo	5.3

III. ACTUALITÉS

1. Le retard d'Apple face à la faille de faceTime

Mardi 29 janvier, Apple a fait la une de l'actualité pour de mauvaises raisons. En créant un appel FaceTime de groupe, il était possible d'entendre son interlocuteur sans que celui-ci réponde. Pire, en cas de manipulation physique de l'appareil, la caméra s'activait par elle-même. N'importe quel iPhone pouvait donc servir de mouchard... depuis trois mois. Dans l'urgence, Apple a désactivé les serveurs de FaceTime de groupe, en attendant une mise à jour corrective d'iOS.

https://www.01net.com/actualites/l-incroyable-retard-d-apple-pour-corriger-le-bug-de-facetime-1622974.html

2. Facebook a payé des utilisateurs pour les espionner

Selon une longue enquête de TechCrunch, Facebook a utilisé pour cela trois services offrant aux internautes de participer à des tests (Applause, BetaBound et uTest), histoire de masquer sa présence. Tout cela dans le cadre de ce que Facebook nomme en interne le « Project Atlas ». Ce dernier a pour but d'identifier les tendances d'utilisation des smartphones dans le monde entier. Un moyen de prendre le pas sur ses concurrents. C'est par exemple grâce à l'application VPN Onavo – depuis retirée de l'App Store par Apple – que Facebook avait identifié l'explosion de l'usage de WhatsApp avant de racheter la société.

https://www.01net.com/actualites/facebook-a-paye-des-utilisateurs-pour-les-espionner-via-leur-smartphone-1622948.html

3. La France livre des PC vérolés au Sénégal

Une petite dizaine de documents confidentiels publiés par The Intercept, et provenant du fond documentaire d'Edward Snowden, montrent que les services secrets américains redoutent depuis presque dix ans des *« piratages subtils »* des produits informatiques fabriqués en Chine. Pourquoi ? Car ce type d'attaque permettrait de compromettre de manière efficace les ordinateurs les plus sensibles dans leurs réseaux gouvernementaux, même ceux qui sont totalement déconnectés (« *air-gapped* »)

https://www.01net.com/actualites/la-dgse-a-livre-des-ordinateurs-veroles-au-senegal-1619657.html

4. Se connecter avec Facebook : le mauvais reflexe

Certains d'entre nous s'en serviront aveuglément et inconditionnellement au quotidien pour publier des photos de leurs récents voyages dans des lieux idylliques, partager des moments marquants, voire bombarder leurs abonnés avec des publications sur leurs habitudes alimentaires. Les autres s'éloigneront de la plateforme par peur, méfiance, confusion, ou par crainte de ce qui pourrait arriver avec les gigantesques quantités de données collectées par Facebook sur ses utilisateurs. Quelle que soit votre position sur le sujet, il est indéniable que depuis sa création en 2004, le réseau social a lentement diminué la capacité de concentration des consommateurs. Mais à quel prix ?

https://www.undernews.fr/authentification-biometrie/se-connecter-avec-facebook-le-mauvais-reflexe.html

5. L'iran lance des attaques chaque jour des attaques contre Israël

« Les cyberattaques de l'Iran se produisent tous les jours. Nous les surveillons, nous les voyons et les déjouons toujours », a affirmé M. Netanyahu. Il avait affirmé au début du mois que son pays était « prêt à tout scénario » à la suite d'informations sur une possible « cyber-intervention » étrangère lors des élections législatives du 9 avril

https://fr.timesofisrael.com/netanyahu-liran-lance-tous-les-jours-des-cyber-attaques-contre-israel/

6. Phishing Campaign Delivers Nasty Ransomware,

Une campagne, remarquée par des chercheurs de Carbon Black, a frappé les systèmes infectés avec une combinaison d'attaques mortelles qui permet de recueillir les informations d'identification, de collecter des informations sur le système et les processus, puis de crypter des données afin d'extorquer des paiements aux victimes. L'attaque a été lancée à l'origine via des courriels de phishing contenant un document Word joint avec des macros incorporées. La macro appelle ensuite un script PowerShell codé et utilise une série de techniques pour télécharger et exécuter une souche de logiciels malveillants Ursnif et une variante du ransomware GandCrab.

https://threatpost.com/phishing-gandcrab-ursnif/141182/

7. Cameroon Tribune piraté

Le site web de Cameroon Tribune a été cible d´une attaque cybernétique cette nuit suivant le constat que nous avons effectué sur les lieux. L´attaque a été perpétrée par le groupe Anonymous , réputé dans le monde pour des actions semblables pour des causes diverses. Cependant la réaction du quotidien se s´est pas fait attendre. Le site est de nouveau accessible avec les contenus appropriés.

https://www.camerounweb.com/CameroonHomePage/NewsArchive/Le-site-web-du-gouvernement-Cameroon-tribune-victime-d-une-cyberattaque-455056

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**.