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 d'Avril 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 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. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • Ubuntu 12.04 ESM • Ubuntu 14.04 LTS • Ubuntu 16.04 LTS • Ubuntu 18.04 LTS • Ubuntu 18.10	03/04/2019	CVE-2019-3819	Ubuntu 18.04.02 LTS	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3933-2/	10.0
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et un problème de sécurité non spécifié par l'éditeur. Systèmes affectés ; Google Android toutes versions n'intégrant pas le correctif de sécurité du 01 avril 2019.	02/04/2019	CVE-2019-2245	Android 9 : Pie	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2019-04-01.html	10.0

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 un déni de service, et un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Module for Live Patching 15	03/04/2019	CVE-2019-9213	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20190845-1/	10.0
Vulnérabilité dans Apple macOS	De multiples vulnérabilités ont été découvertes dans Apple macOS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : • macOS 10.13 High Sierra versions antérieures à 17G6030 • macOS 10.12 Sierra versions antérieures à 16G1918	01/04/2019	CVE-2019-9213	Contacter Apple	Veuillez-vous référer au Bulletin de sécurité https://support.apple.com/en-us/HT209635	10.0

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Plusieurs vulnérabilités ont été corrigées dans le CMS Drupal. Un attaquant distant pourrait exploiter une de ces vulnérabilités pour obtenir ou modifier des informations sensibles. Les versions affectées sont les suivantes : • Drupal 8.4.X version antérieure à 8.4.5, • Drupal 7.X version antérieure à 7.57	05/04/2019	–	8.6.14 Télécharger	Mettre à jour le CMS	8.5

II.3 SERVEUR WEB

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité serveur du web Apache HTTP	Apache software foundation annonce la disponibilité d'une mise à jour qui permet de corriger plusieurs vulnérabilités au niveau du serveur web Apache HTTP. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'élévation de privilèges, le contournement de la politique de sécurité ou le déni de service. Les systèmes infectés sont les suivants : • Serveur web Apache HTTP version 2.4.x antérieures à la version 2.4.39	22/03/2019	CVE-2019-0211 CVE-2019-0217 CVE-2019-0215 CVE-2019-0197 CVE-2019-0196 CVE-2019-0220	2.4.39 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://httpd.apache.org/security/vulnerabilities_24.html	5.2
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. Les systèmes affectés sont les suivants : • PHP versions 7.1.x antérieures à 7.1.28	04/04/2019	CVE-2019-11034 CVE-2019-11035	7.1.28 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.php.net/ChangeLog-7.php	3.1

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits VMware	Plusieurs vulnérabilités ont été corrigées dans les produits VMware. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • VMware Fusion pour OSX versions 11.x antérieures à 11.0.3 • VMware Fusion pour OSX versions 10.x antérieures à 10.1.6 • VMware Workstation versions 15.x antérieures à 15.0.3 • VMware Workstation versions 14.x antérieures à 14.1.6 • VMware ESXi versions 6.7 antérieures à ESXi670-201903001	29/03/2019	CVE-2019-5524	Contacter VMware	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.vmware.com/security/advisories/VMSA-2019-0005.html	7.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Elles permettent à un attaquant de provoquer un déni de service à distance et une élévation de privilèges. Les versions vulnérables sont : • FortiOS versions antérieures à 6.2.0 • FortiSandbox versions antérieures à 3.0.0	03/04/2019	CVE-2018-1356	Contacter Fortinet	Veuillez-vous référer au bulletin de sécurité https://fortiguard.com/psirt/FG-IR-18-024	6.2
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 un déni de service à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les systèmes infectés sont les suivants : • IBM Spectrum Protect Snapshot (anciennement Tivoli Storage FlashCopy Manager) pour VMware versions antérieures à 4.1.6.7 • IBM Watson Compare and Comply versions antérieures à V1.1.4 Magento 2.3 versions antérieures à 2.3.1	27/03/2019	CVE-2018-10237	Contacter IBM	Veuillez-vous référer au bulletin de sécurité https://www-01.ibm.com/support/docview.wss?uid=ibm10876202	5.3

III. ACTUALITÉS

1. Renoncer à une mise à jour de sécurité par peur d'impact sur l'activité

La nouvelle étude « Resilience Gap » publiée aujourd'hui par Tanium révèle des lacunes inquiétantes quant à la capacité de résilience des entreprises à travers le monde, mais aussi en France. Dans un contexte où le nombre et la complexité des cyberattaques augmentent de concert, la visibilité et le contrôle, en temps réel, de l'architecture informatique deviennent fondamentaux pour les entreprises. En effet, seule une connaissance fiable et immédiate des actifs informatiques et des processus opérationnels de l'entreprise, permettra à un dirigeant de prendre rapidement les bonnes décisions et de rétablir l'activité en état de fonctionnement normal.

https://www.undernews.fr/reseau-securite/94-des-dsi-et-rssi-francais-ont-deja-renonce-a-une-mise-a-jour-de-securite-par-peur-de-limpact-sur-lactivite-commerciale.html

2. Antivirus xiaomi piratés

Les chercheurs en sécurité de Check Point Software ont révélé une faille critique dans Guard Provider, l'antivirus préinstallé des smartphones Xiaomi. Ce logiciel intègre trois moteurs antivirus – Avast, AVL, Tencent – parmi lesquels l'utilisateur peut en activer un. Mais les mises à jour de ces moteurs antivirus ne sont pas téléchargées au travers d'une connexion chiffrée. Un pirate qui se trouve sur le même réseau pourrait donc altérer les données reçues par Guard Provider. Et comme ces trois moteurs antivirus partagent le même espace mémoire et que l'intégrité des mises à jour n'est pas vérifiée à 100 %, les chercheurs ont montré qu'il était possible de faire exécuter n'importe quel code malveillant sur le terminal.

https://www.01net.com/actualites/les-smartphones-xiaomi-pouvaient-etre-pirates-via-leur-antivirus-1667363.html

3. Des données de Facebook en accès libre sur le web

Les chercheurs en sécurité de la société UpGuard ont trouvé deux espaces de stockages Amazon S3 ouverts à tous et contenant d'énormes quantité de données provenant d'utilisateurs Facebook. Le premier espace appartenait à Cultura Colectiva, une société mexicaine. Il contenait plus de 540 millions de données enregistrées : noms, identifiants Facebook, commentaires, réactions, likes, etc. Le second espace était lié à « At the pool », une application intégrée au réseau social Facebook. Il contenait les données de plus de 22 000 utilisateurs Facebook : noms, emails, goûts musicaux, photos, évènements, groupes, intérêts, amis, etc. On pouvait même y trouver des mots de passe stockés en clair, qui étaient probablement ceux de l'application. Les deux espaces de stockage ont, depuis, été déconnectés.

https://www.01net.com/actualites/des-centaines-de-millions-de-donnees-d-utilisateurs-facebook-etaient-en-acces-libre-sur-le-web-1666424.html

4. Google fait le ménage dans son écosystème

Dans la cinquième édition du rapport annuel sur la sécurité d'Android, que Google vient de publier, il y a à la fois une bonne et une mauvaise nouvelle. La bonne nouvelle, c'est que le géant informatique continue d'améliorer le niveau de sécurité du système d'exploitation et l'efficacité de ses dispositifs de protection. Avec la dernière version Android Pie, le taux d'infection n'est plus que de 0,18 % contre 0,65 % et 0,55 % pour respectivement Lollipop et Marshmallow.

https://www.01net.com/actualites/pour-securiser-android-google-est-force-de-faire-la-police-dans-son-ecosysteme-1665793.html

5. Un malware pour truquer des scans de tumeurs

Des chercheurs israéliens sont parvenus à développer un logiciel malveillant capable d'altérer les résultats d'un scanner médical afin d'afficher ou de supprimer des cellules cancéreuses très facilement. Mais leurs recherches mettent avant tout en exergue la vétusté des infrastructures hospitalières face aux risques de cyberattaques.

https://cyberguerre.numerama.com/1169-cybersecurite-des-hopitaux-des-chercheurs-ont-cree-un-malware-pour-truquer-des-scans-de-tumeurs-cancereuses.html?utm_medium=distibuted&utm_source=rss&utm_campaign=1169

6. La police Britannique offre des emplois aux cyber délinquants

Bluescreen IT est une société de cybersécurité située à Plymouth dans le sud-ouest de l'Angleterre et qui a un lien très particulier avec la police pour trouver des pirates qui ont besoin d'orientation. En effet, Bluescreen IT emploie des pirates informatiques jugés dignes d'une seconde chance par les autorités, qui opposent leur intelligence à certains des criminels en ligne anonymes qu'ils considéraient comme des frères d'armes. Ces jeunes ont tous été accusés de crimes graves, mais au lieu d'être jugés par le système de justice pénale, ils se sont vu offrir une seconde chance

ttps://securite.developpez.com/actu/255157/La-police-britannique-offre-aux-hackers-adolescents-des-emplois-de-seconde-chance-dans-la-cybersecurite-une-initiative-a-encourager/

7. Mise à jour urgente d'apache http server

Les responsables de l'un des serveurs web les plus populaires au monde, Apache HTTP Server, ont corrigé une vulnérabilité critique qui aurait pu fournir à un attaquant le moyen d'obtenir un contrôle type administrateur "root" complet sur des systèmes Unix.

https://news.sophos.com/fr-fr/2019/04/05/carpe-diem-mise-a-jour-urgente-apache-http-server/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SophosFranceBlog+%28Sophos+News+FR%29

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. Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
4. 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.
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**.