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 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 Mozilla Firefox	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 : Firefox versions antérieures à 66.0.4 Mozilla Firefox ESR version antérieure à 60,6.2.	06/05/2019		66.0.4 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Google Chrome	Google vient de publier une mise à jour de sécurité qui permet de corriger plusieurs vulnérabilités dans le navigateur Google chrome. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'accéder à des données confidentielles. Systèmes affectés : Google chrome antérieures à 74.0.3729.131 sur Windows, Linux et Mac.	02/05/2019		74.0.3729.131 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 Google Android	Plusieurs vulnérabilités ont été corrigées dans Google Android. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Google Android toutes versions n'intégrant pas le correctif de sécurité du 06 Mai 2019	09/05/2019	CVE-2019-2259	-	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2019-05-01.html	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. Les versions infectées sont les suivantes : Google Chrome OS versions antérieures à 74.0.3729.125 (Platform version: 11895.95.0/1)	02/05/2019		74.0.3729.125 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/05/stable-channel-update-for-chrome-os.html	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Une vulnérabilité a été découverte dans Drupal. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Drupal versions 8.7 antérieures à 8.7.1 • Drupal versions 8.6 antérieures à 8.6.16 • Drupal versions 7 antérieures à 7.67 • Drupal versions 8 antérieures à 8.6.x	09/05/2019	CVE-2019-11831	8.7.1 Télécharger	Mettre à jour le CMS	8.5
Vulnérabilité dans le CMS Joomla	De multiples vulnérabilités ont été découvertes dans Joomla! Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Joomla! versions 1.7.0 à 3.9.5	09/05/2019	CVE-2019-11809	3.9.6 Télécharger	Mettre à jour le CMS	8.1

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans IBM WebSphere Application Server	Une vulnérabilité a été découverte dans IBM WebSphere Application Server. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes infectés sont les suivants : • IBM Tivoli Storage Productivity Center versions 5.2.0 à 5.2.7.1 • IBM Spectrum Control versions 5.2.8 à 5.2.17.2 • IBM Spectrum Control versions 5.3.0 à 5.3.1	09/05/2019	CVE-2018-10237	Contacter IBM	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www-01.ibm.com/support/docview.wss?uid=ibm10871890	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits Kaspersky Lab	Kaspersky Lab annonce la correction d'une vulnérabilité affectant plusieurs de ses produits. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire avec des privilèges élevés. Les systèmes infectés sont les suivants : Produits de KasperSky utilisant la base de données d'antivirus ; versions antérieures aux versions de la mise à jour du 4 avril 2019.	13/05/2019	CVE-2019-8285	Contacter Kaspersky	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://support.kaspersky.com/vulnerability.aspx?el=12430#080519	7.3
Vulnérabilité dans SQLite3	Une vulnérabilité a été corrigée dans SQLite3. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code arbitraire à distance. Les systèmes infectés sont les suivants : SQLite3 version antérieure à 3.28.0	13/05/2019	CVE-2019-5018	3.28.0 Télécharger	Veuillez-vous référer au guide de sécurité https://www.sqlite.org/src/info/884b4b7e502b4e99	7.9

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. Les systèmes affectés sont les suivants : • PHP versions 7.2.x antérieures à 7.2.18 • PHP versions 7.3.x antérieures à 7.3.5 • PHP versions 7.1.x antérieures à 7.1.29	02/05/2019		7.3.5 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.php.net/ChangeLog-7.php#7.1.29	5.1
Vulnérabilité dans Dell supportAssist	Une vulnérabilité a été détectée dans les ordinateurs utilisant l'utilitaire 'Dell supportAssist' qui est préinstallé sur la plupart des machines de la marque Dell. L'exploitation de cette faille peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions vulnérables sont : Dell SupportAssist versions antérieures à 3.2.0.90	03/05/2019	CVE-2019-3719	Contacter DELL	Veuillez-vous référer au bulletin de sécurité https://www.dell.com/support/article/ma/fr/madhs1/sln316857/dsa-2019-051-vuln%C3%A9rabilit%C3%A9s-de-plusieurs-clients-dell-supportassist?lang=fr	3.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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. Les systèmes affectés sont les suivants : • Cisco IOS XR 64-bit versions antérieures à 6.5.3 et 7.0.1 • Cisco Nexus 9000 Series ACI Mode Switch versions antérieures à 14.1(1i) • Cisco AsyncOS versions 11.7.x antérieures à 11.7.0-406 • Cisco ASA versions 9.10.x antérieures à 9.10.1.17 • Cisco Firepower et FMC versions 6.3.x antérieures à 6.3.0.3 (sortie prévue pour la semaine du 6 mai 2019) • Cisco Small Business 200 Series Smart Switches et Small Business 300 Series et 500 Series Managed Switches versions antérieures à 1.4.10.6	01/05/2019	CVE-2019-1859	Contacter CISCO	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-hw-clock-util	4.5

III. ACTUALITÉS

1. Les équipes de la plateforme de messagerie instantanée WhatsApp ont récemment découvert une faille majeure

Un logiciel espion, créé par un "acteur aux technologies avancées", s'est servi d'une faille dans l'application de messagerie instantanée WhatsApp pour prendre le contrôle des téléphones portables, affirme le Financial Times. Un correctif supprimant la brèche a été déployé lundi 13 mai.

https://www.france24.com/fr/20190514-whatsapp-espionnage-faille-securite-nso-israel

2. Les codes sources de trois antivirus en vente sur le dark web

Et si, derrière votre bel antivirus, se planquait en réalité un groupe de pirates ? L'idée est loin d'être absurde, car les codes sources de trois antivirus américains sont actuellement en vente sur le Dark Web. Selon les analystes de la société AdvIntel, un groupe de pirates baptisé Fxmsp propose 30 To de données volées auprès de trois éditeurs antivirus majeurs, basés aux Etats-Unis

https://www.01net.com/actualites/les-codes-sources-de-trois-antivirus-sont-en-vente-sur-le-dark-web-1689406.html

3. Le smartphone devient votre pièce d'identité

Présenté à l'occasion de la conférence Googe I/O 2019, le nouveau système d'exploitation Android Q ne bénéficiera pas seulement de nouvelles fonctionnalités mais aussi de nouvelles protections. Ainsi, le chiffrement des données personnelles deviendra une obligation, quel que soit le type de terminal :

https://www.01net.com/actualites/android-q-renforcera-la-securite-de-vos-donnees-et-veut-faire-de-votre-smartphone-une-piece-d-identite-1689191.html

4. Israël répond par des missiles à une cyberattaque

Comment réagir quand on est confronté à une cyberattaque ? Cette question taraude bon nombre de pays depuis des années. Israël vient de marquer les esprits en apportant une réponse assez radicale. Ciblées par une cyberattaque du Hamas, les forces de défense israéliennes ont répliqué avec des missiles pour détruire le site à partir duquel les hackers lançaient leurs opérations. D'après l'armée israélienne, cette contre-attaque fut un succès.

https://www.01net.com/actualites/cible-par-une-cyberattaque-israel-repond-avec-des-missiles-1686248.html

5. Une faille de sécurité révèle un nouveau Big Brother

Ceux qui se demandaient à quoi peut bien ressembler un système de surveillance dans une ville chinoise sont désormais servis. Les données d'un tel système étaient librement accessibles en ligne depuis un navigateur web, sans aucun contrôle d'accès. Elles ont été trouvées par le chercheur en sécurité John Wethington, qui a collaboré avec TechCrunch pour contacter le fournisseur impliqué et publier les informations qui en découlent.

https://www.01net.com/actualites/chine-une-faille-de-securite-donne-un-apercu-d-un-systeme-de-surveillance-digne-de-big-brother-1686365.html

6. Le malware Electricfish

Le FBI et le DHS annoncent avoir découvert un nouveau malware utilisé par les hackers du groupe nord-coréen Lazarus pour exfiltrer les données de leurs victimes. Selon le MAR (malware analysis report) AR19-129A publié sur le site web US-CERT du gouvernement américain, ce malware intitulé ELECTRICFISH a été détecté en suivant les activités malveillantes du groupe de hackers Lazarus, soutenu par le gouvernement de Corée du Nord, et aussi connu sous le nom de HIDDEN COBRA, Guardians of Peace, ZINC ou encore NICKEL ACADEMY.

https://www.lebigdata.fr/coree-du-nord-electricfish

7. Révolution des usages pour les Botnets

Les acteurs malveillants créent toujours de nouvelles astuces pour rendre les botnets de plus en plus multifonctionnels et extrêmement volatiles. Tribune par Alain Khau, Spécialiste Cybersécurité EMEA, CenturyLink – A titre d'exemple, le botnet « TheMoon », qui existe depuis 2014, exploite les failles de sécurité et prends le contrôle de routeurs vulnérables et de périphériques IoT pour lancer des attaques DDoS. Mais dernièrement, un nouveau module a été ajouté au botnet, permettant à l'auteur du botnet de vendre ou de louer son réseau proxy comme un service et ainsi donner la possibilité à d'autres acteurs malveillants de l'utiliser pour lancer des attaques par force brute, obfusquer le trafic ou pour déployer un système de fraude publicitaire vidéo.

https://www.undernews.fr/hacking-hacktivisme/les-botnets-une-revolution-des-usages.html

8. Attention aux fausses barres d'adresse dans chrome

Un développeur a mis au point un système permettant d'afficher une fausse barre d'adresse dans le navigateur de Google pour Android. Cela pourrait permettre à des escrocs de rendre de faux sites encore plus réalistes.

https://www.01net.com/actualites/phishing-attention-a-cette-fausse-barre-d-adresse-dans-chrome-1682318.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. 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**.