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 d'Août 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 un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont : Chrome, versions antérieures à 76.0.3809.132	27/08/2019	CVE-2019-5869	76.0.3809.132 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une exécution de code arbitraire et un déni de service. Les systèmes affectés sont : • Firefox versions antérieures à Firefox 69 • Firefox ESR versions antérieures à Firefox ESR 68.1 • Firefox ESR versions antérieures à Firefox ESR 60.9	04/09/2019	CVE-2019-11753	69 Télécharger	Mettre à jour le navigateur	10.0

Vulnérabilité dans Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité et une exécution de code à distance. Les systèmes concernés sont les suivants : • Internet Explorer 10 • Internet Explorer 11 • Internet Explorer 9	14/08/2019	CVE-2019-1192	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	14/08/2019	CVE-2019-1197	-	Mettre à jour via Windows Update	9.0

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 un déni de service, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Server for SAP 12-SP1 • SUSE Linux Enterprise Server 12-SP1-LTSS • SUSE Linux Enterprise Module for Public Cloud 12 • SUSE OpenStack Cloud Crowbar 8 • SUSE OpenStack Cloud 8 • SUSE Linux Enterprise Server for SAP 12-SP3 • SUSE Linux Enterprise Server 12-SP3-LTSS • SUSE Linux Enterprise Server 12-SP3-BCL • SUSE Linux Enterprise High Availability 12-SP3 • SUSE Enterprise Storage 5 • SUSE CaaS Platform 3.0 • HPE Helion Openstack 8	02/09/2019	CVE-2019-15118	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20192262-1/	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 de provoquer un déni de service et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Ubuntu 19.04 • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS	03/09/2019	CVE-2019-15292	19.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4118-1/	10.0
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les versions affectées sont les suivantes : • Debian stretch versions antérieures à 4.9.168-1+deb9u5 • Debian buster versions antérieures à 4.19.37-5+deb10u2	14/08/2019	CVE-2019-14284	10.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.debian.org/security/2019/dsa-4497	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, un déni de service à distance et une atteinte à la confidentialité des données. La version affectée est la suivante : Android version Q sans le correctif de sécurité 2019-09-01	21/08/2019	CVE-2019-9459	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/android-q.html	10.0

Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une exécution de code à distance, une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service et un contournement de la fonctionnalité de sécurité.	13/08/2019	CVE-2019-1227	10	Mettre à jour le système via Windows Update	10.0

II.1 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans WordPress	De multiples vulnérabilités ont été découvertes dans WordPress. Elles permettent à un attaquant de provoquer : un contournement de la politique de sécurité une injection de code indirecte à distance (XSS) une injection de requêtes illégitimes par rebond (CSRF). Les versions affectées sont les suivantes : WordPress versions antérieures à 5.2.3	05/09/2019		5.2.3 Télécharger	Mettre à jour le CMS	8.1

II.2 AUTRES

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 contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les versions vulnérables sont les suivantes : • Cisco IND versions antérieures à 1.6.0 • Cisco Webex Teams versions antérieures à 3.0.12427.0 pour Windows	05/09/2019	CVE-2019-1976	-	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ind	8.8
Vulnérabilité dans SAMBA	Une vulnérabilité a été découverte dans Samba. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les versions vulnérables sont : Samba versions antérieures à 4.9.0	03/09/2019	CVE-2019-10197	4.9.0 Télécharger	Veuillez-vous référer au bulletin de sécurité https://www.samba.org/samba/security/CVE-2019-10197.html	6.2

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 exécution de code à distance et un contournement de la fonctionnalité de sécurité.	14/08/2019	CVE-2019-1229	-	Effectuez une mise à jour via Windows Update	10.0
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.	14/08/2019	CVE-2019-1205	2019	Mettre à jour le système via Windows Update	7.7
Vulnérabilité dans Libreoffice	De multiples vulnérabilités ont été découvertes dans Libreoffice. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : Libreoffice versions 6.3.x antérieures à 6.3.1	06/09/2019	CVE-2019-9855	6.3.1 Télécharger	Veuillez-vous référer au bulletin de sécurité https://www.libreoffice.org/about-us/security/advisories/cve-2019-9855/	3.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Nagios	De multiples vulnérabilités ont été découvertes dans Nagios. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Nagios Core versions antérieures à 4.4.5	21/08/2019	-	4.4.5 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.nagios.org/projects/nagios-core/history/4x/	6.3
Vulnérabilité dans les produits Kaspersky	Une vulnérabilité a été découverte dans les produits Kaspersky. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les systèmes infectés sont les suivants : • Kaspersky Anti-Virus 2019 versions antérieures à Patch E • Kaspersky Internet Security 2019 versions antérieures à Patch E • Kaspersky Total Security 2019 versions antérieures à Patch E • Kaspersky Free Anti-Virus 2019 versions antérieures à Patch E	16/08/2019		Contacter Kaspersky	Veuillez-vous referez au Bulletin de sécurité de l'éditeur https://support.kaspersky.com/general/vulnerability.aspx?el=12430#160819	10.0

III. ACTUALITÉS

1. Failles de sécurité dans les traceurs GPS

Avast, l'un des leaders des produits de sécurité digitale, a découvert de sérieuses failles de sécurité dans le T8 Mini GPS tracker et dans près de 30 autres modèles du même fabricant, Shenzhen i365 Tech. Commercialisés pour garantir la sécurité des enfants, des personnes âgées, des animaux domestiques et même des biens personnels, ces appareils dévoilent toutes les données envoyées dans le cloud, y compris les coordonnées GPS exactes en temps réel.

https://www.undernews.fr/alertes-securite/avast-decouvre-des-failles-de-securite-dans-des-traceurs-gps-plus-dun-demi-million-denfants-et-de-personnes-agees-concernes.html

2. Plus de 950 millions de données internautes exposées

Données d'internautes dans les mains de pirates ! Le black market explose de propositions commerciales malveillantes. Données bancaires, ventes de médicaments contrefaits (ou pas), documents administratifs (carte vitale, fiche de paie, facture, contrat, …) et autres bases de données piratées de par le monde. Des espaces pirates qui créés de « l'emploi » et des « nouveaux métiers » du cybercrime.

https://www.zataz.com/decouverte-de-950-millions-de-donnees-dinternautes/

3. Apple offre un million $ de récompense pour trouver des failles dans leurs équipements.

Même les services de renseignement les plus réputés du monde peuvent essuyer des cyberattaques à succès. Le FSB, successeur du KGB soviétique, fait partie de cette catégorie, bien que l'institution en elle-même n'a pas directement été ciblée. C'est en effet l'un de ses prestataires, SyTech en l'occurrence, qui a subi le courroux du groupe de hackers 0v1ru$, nous apprend BBC Russie.

https://cyberguerre.numerama.com/1601-piratage-du-fsb-sur-quels-projets-travaillent-les-services-de-renseignement-russes.html

4. Leaky server exposes 419 million phone numbers of facebook users

Selon un rapport publié, le serveur, dépourvu de protection par mot de passe, contenait plus de 419 millions d'enregistrements dans plusieurs bases de données d'utilisateurs Facebook, répartis sur plusieurs zones géographiques - y compris 133 millions d'enregistrements d'utilisateurs basés aux États-Unis. Dix-huit millions d'enregistrements d'utilisateurs au Royaume-Uni et de 50 millions d'utilisateurs basés au Vietnam ont également été conservés sur le serveur.

https://threatpost.com/leaky-server-exposes-419m-phone-numbers-of-facebook-users/148029/

5. Simuler des voix pour arnaquer

Une entreprise britannique du secteur de l'énergie a été victime d'une variante inédite et perfectionnée de « l'arnaque au président ». Ce type d'escroquerie, rappelons-le, consiste à se faire passer pour le dirigeant d'une société et de susciter des virements urgents vers de comptes en banque contrôlés par les malfrats. Dans le cas présent, révélé par The Wall Street Journal et relayé par Gizmodo, les escrocs se sont appuyés sur un système d'intelligence artificielle pour générer une simulation presque parfaite de la voix du PDG de la maison mère allemande. Dans le domaine de l'intelligence artificielle, ce type de simulation est également appelée « deep fake ».

https://www.01net.com/actualites/ils-arnaquent-une-entreprise-en-simulant-la-voix-de-son-pdg-grace-a-une-ia-1760456.html

6. Amazon : un énorme réseau de vidéosurveillance

Avec ses caméras de vidéosurveillance Ring, Amazon est désormais très bien placé pour gagner aux prochains Big Brother Awards. Depuis mars 2018, les cadres de Ring font la tournée des services de police aux États-Unis, pour les inciter à devenir partenaires de « Neighbors », un réseau social dédié à la surveillance locale, entre voisins. Cette application permet aux membres de partager des informations et, surtout, des vidéos enregistrées par les caméras Ring. L'objectif étant de signaler les évènements louches ou d'aider la résolution de délits : vols de colis, cambriolages de maisons, effractions de voitures, violences, etc.

https://www.01net.com/actualites/les-cameras-ring-d-amazon-discretement-transformees-en-un-enorme-reseau-de-videosurveillance-1757458.html

7. Plus facile de pirater un iPhone qu'un Android

Les temps changent. Spécialisée dans la vente d'attaques informatiques, l'entreprise Zerodium vient de mettre à jour sa liste de prix, et pour la première fois le piratage de smartphones Android est mieux rémunéré que celui de l'iPhone. Un hacker qui trouve une méthode complète de piratage sur Android, avec persistance et sans aucune interaction avec l'utilisateur (« zéro-clic »), peut désormais gagner jusqu'à 2,5 millions de dollars. Celui qui trouve une méthode équivalente sur iPhone, en revanche, ne pourra espérer « que » 2 millions de dollars.

https://www.01net.com/actualites/il-est-desormais-plus-complique-de-pirater-un-smartphone-sous-android-qu-un-iphone-1760934.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**.