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 Juillet 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	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, un déni de service à distance et un contournement de la politique de sécurité. Les versions concernées sont les suivantes : Firefox versions antérieures à 68.0	10/07/2019	CVE-2019-11730	68.0 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Microsoft Internet Explorer	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une exécution de code à distance. Les systèmes infectés sont les suivants : • Internet Explorer 11 • Internet Explorer 10 • Internet Explorer 9	10/07/2019	CVE-2019-1104	11	Mettre à jour via Windows Update	9.0

Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une élévation de privilèges et une exécution de code à distance.	10/07/2019	CVE-2019-1107	-	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 Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité, une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service et une exécution de code à distance.	10/07/2019	CVE-2019-1130	10	Mettre à jour le système via Windows Update	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 contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : Google Android toutes versions n'intégrant pas le correctif de sécurité du 01 juillet 2019	27/06/2019	CVE-2019-2386	Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2019-07-01.html	10.0

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 la confidentialité des données, et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • SUSE OpenStack Cloud 7 • SUSE Linux Enterprise Server for SAP 12-SP2 • SUSE Linux Enterprise Server 12-SP2-LTSS • SUSE Linux Enterprise Server 12-SP2-BCL • SUSE Enterprise Storage 4 • SUSE Linux Enterprise Module for Public Cloud 15 • SUSE Linux Enterprise Module for Open Buildservice Development Tools 15-SP1	15/07/2019	CVE-2019-12819	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20191823-2/	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Joomla	Une vulnérabilité a été découverte dans Joomla. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : Joomla! versions antérieures à 3.9.9	10/07/2019		3.9.9 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 les produits Intel	De multiples vulnérabilités ont été découvertes dans les produits Intel. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Les versions affectées sont les suivantes : • Intel SSD DC S4500 Series versions antérieures à SCV10150 • Intel SSD DC S4600 Series versions antérieures à SCV10150 • Intel Processor Diagnostic Tool pour 32-bit versions antérieures à 4.1.2.24_32bit • Intel Processor Diagnostic Tool pour 64-bit versions antérieures à 4.1.2.24_64bit	10/07/2019	CVE-2019-11133	-	Veuillez-vous référer au Bulletin de sécurité https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00268.html	9.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Squid	De multiples vulnérabilités ont été découvertes dans Squid. 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 versions affectées sont les suivantes : Squid versions antérieures à 4.8	15/07/2019	CVE-2019-13345	4.8 Télécharger	Veuillez-vous référer au guide suivant http://www.squid-cache.org/Advisories/SQUID-2019_6.txt	4.1
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.	10/07/2019	CVE-2019-1137	-	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 atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	10/07/2019	CVE-2019-1134	2019	Mettre à jour le système via Windows Update	7.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Cisco ASA et FTD	De multiples vulnérabilités ont été découvertes dans Cisco ASA et FTD. Elles permettent à un attaquant de provoquer un déni de service à distance. Les systèmes infectés sont les suivants : • Cisco ASA versions antérieures à 9.4.4.36 • Cisco ASA versions 9.5.x et 9.6.x antérieures à 9.6.4.29 • Cisco ASA versions 9.7.x et 9.8.x antérieures à 9.8.4.3 • Cisco ASA versions 9.9.x antérieures à 9.9.2.52 • Cisco ASA versions 9.10.x antérieures à 9.10.1.22 • Cisco ASA versions 9.12.x antérieures à 9.12.2 • Cisco FTD versions antérieures à 6.2.3.13 • Cisco FTD versions 6.3.x antérieures à 6.3.0.4 • Cisco FTD versions 6.4.x antérieures à 6.4.0.2	11/07/2019	CVE-2019-1873	Contacter CISCO	Veuillez-vous référer au guide suivant https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190710-asa-ftd-dos	8.0

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 élévation de privilèges, une exécution de code à distance, une usurpation d'identité et un déni de service.	10/07/2019	CVE-2019-1113	4.8 Télécharger	Effectuez une mise à jour via Windows Update	10.0
Vulnérabilité dans Foxit Reader et PhantomPDF	De multiples vulnérabilités ont été découvertes dans Foxit Reader et PhantomPDF. Elles permettent à un attaquant de provoquer un déni de service à distance et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Foxit PhantomPDF Mac versions antérieures à 3.3 sur macOS • Foxit Reader versions antérieures à 3.3 sur macOS	15/07/2019	-	3.3 Contacter Foxitsoftware	Veuillez-vous référer au bulletin de sécurité https://www.foxitsoftware.com/support/security-bulletins.php	3.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Thunderbird	De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. 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 versions affectées sont les suivantes : Thunderbird versions antérieures à 60.8	12/07/2019	CVE-2019-11730	60.8 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.mozilla.org/en-US/security/advisories/mfsa2019-23/	3.5
Vulnérabilité dans VMware ESXi	Une vulnérabilité a été découverte dans VMware ESXi. Elle permet à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • ESXi version 6.7 • ESXi version 6.5 versions antérieures à ESXi650-201907201-UG	10/07/2019	CVE-2019-5528	6.7 Contacter VMware	Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2019-0011.html	7.7

III. ACTUALITÉS

1. Des millions de nouveaux domaines frauduleux

À l'instar de nombreuses autres méthodes d'attaque très populaires aujourd'hui, la fraude au nom de domaine cible des individus plutôt que des infrastructures en faisant appel à l'ingénierie sociale pour amener les utilisateurs à croire que les domaines auxquels ils accèdent sont légitimes », a déclaré Ali Mesdaq, directeur Digital Risk Engineering. « Du fait du peu d'obstacles à l'enregistrement des noms de domaine et de la facilité d'exécution, il est essentiel que les sociétés restent vigilantes face aux domaines suspects et illégaux susceptibles de présenter un risque pour leur marque et leurs clients.

https://www.zataz.com/fraude-nom-de-domaine/

2. Une mairie préfère payer un chantage numérique

Ransomwares ! Aujourd'hui, dans le monde des pirates informatiques professionnels, on trouve les économistes. Ils étudient leurs cibles. Calculent le coût potentiel des factures d'après attaque que devront payer les entreprises infiltrées. C'est ainsi qu'est né le ransomware de l'économe. Le pirate prend en otage les fichiers de la société et réclame une somme inférieure aux coût des travaux qui devront être mis en place par le malmené pour récupérer ses données, se sécuriser, … C'est ainsi que de nombreuses sociétés (privées et publiques) paient les vilains. Sans parler des clés de déchiffrement qui ne fonctionnent pas. Pour Ryuk, les spécialistes de chez Emisoft indiquent un taux de réussite de 3 à 5% de réussite ! En début d'année, ce ransomware avait perturbé les journaux Los Angeles Times, Chicago Tribune, Baltimore Sun, San Diego Union-Tribune…

https://www.zataz.com/ransomwares-une-mairie-prefere-payer-un-chantage-numerique/

3. Un nouvel exploit zero day pour Windows

Les chercheurs d'ESET ont récemment découvert un exploit Windows de type zero-day utilisé dans le cadre d'une attaque très ciblée en Europe de l'Est. Cet exploit reposait sur une vulnérabilité inédite d'escalade des privilèges locaux sur Windows. ESET a immédiatement signalé le problème aux équipes du centre de réponse aux incidents de Microsoft (MSRC), ce qui a permis à l'éditeur de corriger la vulnérabilité et de publier un correctif. L'exploit ne fonctionnera cependant que sur certaines versions plus anciennes de Windows. À partir de Windows 8, en effet, un processus utilisateur n'est plus autorisé à mapper la page NULL, ce qui est un prérequis nécessaire à la réussite de cette attaque.

https://www.undernews.fr/alertes-securite/eset-decouvre-un-nouvel-exploit-zero-day-pour-windows-utilise-dans-une-attaque-extremement-ciblee.html

4. La nouvelle bombe Zip

Une bombe Zip d'un nouveau genre a été créée, atteignant un ratio de compression de 28 millions. Petits farceurs s'abstenir. Un développeur remet les « bombes Zip » au goût du jour. En utilisant une technique de superposition de fichiers, David Fifield a réussi à créer un fichier avec un ratio de compression de 28 millions, voire 97 millions en utilisant le format Zip64. C'est la première fois que quelqu'un atteint un tel ratio sans utiliser de compression récursive (un fichier Zip inclus dans un fichier Zip, etc.). En d'autres termes, ce fichier « se dilate complètement après un seul tour de décompression ».

https://www.01net.com/actualites/une-fois-decompresse-ce-fichier-zip-de-46-mo-atteint-45-po-1729093.html

5. Des applis Androids qui exfiltrent des données en douce

Ce n'est pas parce qu'on n'a pas le droit de faire quelque chose, que c'est impossible à faire. Sur Android, les applications mobiles reçoivent des droits d'accès pour certaines données sensibles, et pour d'autres non. Cela dépend du besoin applicatif et de la volonté de l'utilisateur. Mais certaines applis contournent ces règles pour exfiltrer des données qu'elles n'avaient pas le droit de lire, probablement dans un but de ciblage publicitaire. Pour contourner les droits d'accès, les développeurs de certaines applications imaginent des astuces parfois assez originales, comme l'extraction des données EXIF des photos pour la géolocalisation.

https://www.01net.com/actualites/comment-des-centaines-d-applis-android-exfiltrent-vos-donnees-personnelles-de-facon-illicite-1728557.html

6. Une faille de plus de 17 ans

Télécharger et ouvrir un fichier HTML douteux n'est pas une bonne idée, en tous les cas si vous utilisez Firefox. Le chercheur en sécurité Bartak Tawily vient de montrer qu'un attaquant peut alors télécharger automatiquement et en douce tous les fichiers contenus dans le répertoire dans lequel se trouve le fichier HTML en question, ainsi que les fichiers des sous-répertoires.Pour prouver l'efficacité de sa technique, il a réalisé une vidéo YouTube dans laquelle la victime reçoit un fichier HTML vérolé par e-mail.

https://www.01net.com/actualites/firefox-une-faille-vieille-de-17-ans-permet-de-voler-des-fichiers-sur-un-pc-1725317.html

7. Mozilla bloque les certificats darkmatter pour risque d'espionnage

Depuis 2017, l'entreprise émirati DarkMatter cherche à acquérir le statut d'autorité racine. Mais compte tenu de ses activités de surveillance et de piratage gouvernemental, Mozilla estime qu'on ne peut pas lui faire confiance.

https://www.01net.com/actualites/mozilla-bloque-les-certificats-de-darkmatter-pour-risque-d-espionnage-1728381.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**.