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 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 3
II. VULNÉRABILITÉS PUBLIÉES 4
II.1 NAVIGATEURS 4
Vulnérabilité dans Google Chrome 4
II.2 SYSTÈMES D'EXPLOITATION 5
Vulnérabilité dans le noyau Linux de RedHat 5
Vulnérabilité dans le noyau Linux d'Ubuntu 5
Vulnérabilité dans le noyau Linux de SUSE 6
II.3 CMS 7
Vulnérabilité dans le CMS Drupal 7
II.4 AUTRES 8
Vulnérabilité dans PHP 8
Vulnérabilité critique dans VLC 8
Vulnérabilité dans les produits Apple 9
Vulnérabilité dans OpenSSL 10
Vulnérabilité dans Cisco Nexus 10
Vulnérabilité dans Foxit PhantomPDF 10
Vulnérabilité dans Oracle Virtualization 11
III. ACTUALITÉS 12
IV. NOTES IMPORTANTES 14

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 et un contournement de la politique de sécurité. Les systèmes affectés sont : Google Chrome toutes versions antérieures à Chrome 76.0.3809.87	31/07/2019	CVE-2019-5862	76.0.3809.87 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 de RedHat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une élévation de privilèges et un déni de service à distance.	30/07/2019	CVE-2019-11810	8 Ootpa	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2019:1973	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 une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : Ubuntu 18.04 LTS	02/08/2019	CVE-2019-11884	19.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4069-2/	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 à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes affectés sont les suivants : • SUSE Linux Enterprise Server 11-SP4-LTSS • SUSE Linux Enterprise Server 11-EXTRA • SUSE Linux Enterprise Debuginfo 11-SP4	22/07/2019	CVE-2019-12614	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-201914127-1/	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 8.7.4	18/07/2019	CVE-2019-6342	8.7.4 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 PHP	Plusieurs vulnérabilités ont été corrigées dans PHP. L'exploitation de ces failles pourrait permettre à un attaquant de provoquer un contournement de la politique de sécurité et de porter atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • PHP versions 7.2.x antérieures à 7.2.21 • PHP versions 7.3.x antérieures à 7.3.8	01/08/2019	CVE-2019-11042	7.3.8 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.php.net/ChangeLog-7.php#7.3.8	9.0
Vulnérabilité critique dans VLC	Une vulnérabilité critique a été identifiée dans le lecteur multimédia VLC. La faille ne nécessite pas de privilèges administrateur ou d'interaction utilisateur et peut être exploitée lorsqu'un utilisateur exécute un fichier multimédia illicite via VLC. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant de provoquer un débordement de mémoire et d'exécuter du code arbitraire à distance. Les versions affectées sont les suivantes : VLC 3.0.7.1 et versions antérieures.	24/07/2019	CVE-2019-13615	3.0.7.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité suivant https://nvd.nist.gov/vuln/detail/CVE-2019-13615	4.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Apple	Apple annonce la correction de plusieurs vulnérabilités affectant certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer l'exécution de code arbitraire à distance, le contournement de la politique de sécurité, l'accès à des données confidentielles ou de causer un déni de service. Les systèmes infectés sont les suivants : ➢ iOS versions antérieures à 12.4 ➢ macOS Mojave versions antérieures à 10.14.5 ➢ macOS Sierra 10.12.6 sans le correctif de sécurité 2019-004 ➢ macOS High Sierra 10.13.6 sans le correctif de sécurité 2019-004 ➢ Safari versions antérieures à 12.1.2 ➢ watchOS versions antérieures à 5.3 ➢ tvOS versions antérieures à 12.4	27/07/2019	CVE-2019-8690	Contacter Apple	Veuillez-vous referez au Bulletin de sécurité de l'éditeur https://support.apple.com/en-us/HT210353	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans OpenSSL	Une vulnérabilité a été découverte dans OpenSSL. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données. Les versions infectées sont les suivantes : OpenSSL versions 1.1.1, 1.1.0 et 1.0.2	31/07/2019	CVE-2019-1552	1.1.1c Télécharger	Veuillez-vous référer au guide suivant https://www.openssl.org/news/secadv/20190730.txt	7.7
Vulnérabilité dans Cisco Nexus	Une vulnérabilité a été découverte dans Cisco Nexus. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance. Les systèmes infectés sont les suivants : • Cisco Nexus 9000 Series ACI Mode Switch versions antérieures à 13.2(7f) • Cisco Nexus 9000 Series ACI Mode Switch versions 14.x	01/08/2019	CVE-2019-1901	-	Veuillez-vous référer au guide suivant https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190731-nxos-bo	8.0
Vulnérabilité dans Foxit PhantomPDF	De multiples vulnérabilités ont été découvertes dans Foxit PhantomPDF. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service. Les versions affectées sont les suivantes : Foxit PhantomPDF versions antérieures à 8.3.11	22/07/2019	-	8.3.11 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 Oracle Virtualization	De multiples vulnérabilités ont été découvertes dans Oracle Virtualization. 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 l'intégrité des données. Les versions affectées sont les suivantes : • Oracle VM VirtualBox versions antérieures à 5.2.32 • Oracle VM VirtualBox versions 6.0.x antérieures à 6.0.10	17/07/2019	CVE-2019-2876	6.0.10 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.oracle.com/technetwork/security-advisory/cpujul2019verbose-5072838.html#OVIR	3.5

III. ACTUALITÉS

1. Apple suspend le programme siri

Apple suspend un programme qui permet à certains sous-traitants d'écouter des enregistrements vocaux Siri suites aux réclamations relatives à la protection de la vie privée. La suspension intervient après la publication dans le quotidien d'information The Guardian, d'un reportage décrivant comment ces sous-traitants écoutent régulièrement des enregistrements vocaux intimes, notamment des trafics de drogue ou des enregistrements de couples ayant des relations sexuelles, afin d'améliorer la précision audio, un processus qu'Apple appelle «grading».

https://threatpost.com/apple-suspends-siri-program-privacy-backlash/146894/

2. Un bug dans Android expose la liste des contacts

De nombreuses applications antivirus gratuites Android populaires ont récemment révélé des failles de sécurité et des problèmes de confidentialité, notamment une vulnérabilité critique qui expose les carnets d'adresses de l'utilisateur et une autre faille sérieuse qui permet aux attaquants de désactiver complètement la protection antivirus. Selon une analyse effectuée par Comparitech auprès de 21 fournisseurs d'antivirus Android, trois des applications testées (VIPRE Mobile, AEGISLAB et BullGuard) présentaient de graves failles de sécurité et sept applications n'ont pas détecté de virus de test. Au total, 47% des fournisseurs testés ont échoué.

https://threatpost.com/critical-bug-android-antivirus/146927/

3. Nouvelle version du malware Pegasus

Il ressort qu'une évolution de ce malware parviendrait à copier des clés d'authentification de services tels que Google Drive, Facebook Messenger ou encore iCloud à partir de téléphones infectés. Bref, c'est comme acheter guitare. Plus on la gratte, et plus on découvre des possibilités ! À la suite de cela, un serveur pourrait ensuite se faire passer pour ledit téléphone, simuler son emplacement géographique et collecter des données cloud telles que l'historique complet des données de localisation de la victime, les messages archivés et les photos pour les plateformes de Google, Facebook, Amazon et Microsoft. La sécurité du cloud est devenue une priorité, et il n'est pas surprenant que des pirates informatiques s'en prennent aux terminaux équipés de clés permettant d'ouvrir des coffres forts numériques.

https://www.zataz.com/malware-pegasus/

4. Les vulnérabilités Urgent 11

Des chercheurs en sécurité ont révélé un lot de rien moins que 11 failles affectant le système d'exploitation temps réel (RTOS) VxWorks. Mais son éditeur Wind River n'appréhende pas le risque de la même manière. Dans leur rapport, les chercheurs indiquent que « six de ces vulnérabilités sont classées comme critiques et permettent l'exécution de code à distance. Les autres vulnérabilités sont classées en déni de service, fuites d'informations ou failles logiques. URGENT/11 est sérieux car il permet aux attaquants de prendre le contrôle d'appareils sans interaction avec l'utilisateur, et même de contourner les systèmes de sécurité périmétrique tels que pare-feu et solutions NAT ». Pour les auteurs du rapport, ces caractéristiques « dévastatrices » sont susceptibles de permettre l'exploitation des vulnérabilités par des vers : « elles peuvent être utilisées pour propager des maliciels dans et au sein de réseaux.

https://www.lemagit.fr/actualites/252467817/Les-vulnerabilites-URGENT-11-affectent-des-millions-dappareils-VxWorks

5. Six nouvelles failles critiques dans iOS

Les chercheurs du Project Zero ont permis à Apple de bétonner six brèches de sécurité dans iOS. Des failles qui auraient pu se monnayer très chers sur le marché noir et faire beaucoup de dégâts.

https://www.01net.com/actualites/des-chercheurs-de-google-ont-decouvert-six-failles-critiques-dans-ios-1740612.html

6. Google continue d'investir dans les outils pour l'armée

Gradient Ventures : ce nom ne vous dit rien et pourtant il a en lui les germes du Skynet de Terminator. Sous ce nom se cache le fonds d'investissement que Google a fondé en 2017 pour financer des projets liés à l'intelligence artificielle. Comme le révèle le site d'enquêtes « The Intercept », ce fond est loin d'être neutre et permet à Google d'avoir les coudées franches en matière de technologies liées à la défense.

https://www.01net.com/actualites/ia-google-continue-d-investir-discretement-dans-des-outils-pour-la-police-et-l-armee-1737594.html

7. FaceApp aspire les données comme Facebook et Snapchat

L'application russe FaceApp, qui permet de voir son visage vieilli, collecte des millions de photos à travers le monde, suscitant l'inquiétude sur l'usage qu'elle en fait. Mais, aussi intrusif qu'il soit, cet usage semble refléter la pratique générale et non un cas isolé.

https://www.01net.com/actualites/oui-faceapp-aspire-vos-donnees-tout-comme-facebook-et-snapchat-1733663.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**.