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 2018

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.

I. VULNÉRABILITÉS PUBLIÉES

II.1 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS JOOMLA	Plusieurs vulnérabilités ont été corrigées dans le CMS Joomla. Un attaquant distant pourrait exploiter ces vulnérabilités afin de provoquer un contournement de la politique de sécurité, une atteinte à l'intégrité des données et une injection de code indirecte à distance (XSS). Les versions concernées sont les suivantes : Jomla Core versions antérieures à 3.8.12.	30/08/2018	CVE-2018-15882	3.8.12 Télécharger	Mettre à jour le CMS	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome OS	Google annonce des vulnérabilités non spécifiées sur Chrome OS versions antérieures à 68.0.3440.118 (Platform version: 10718.88.2)	24/08/2018	–	68.0.3440.118 Télécharger	Effectuez une mise à jour du système	9.0
Vulnérabilité dans le Noyau Linux de RedHat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de RedHat. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : Red Hat Enterprise Linux Server - Extended Life Cycle Support 5 x86_64Ubuntu 16.04 LTS Red Hat Enterprise Linux Server - AUS 5.9 x86_64	30/08/2018	CVE-2018- 3646	4.18.5 Télécharger	Effectuez une mise à jour du système	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 une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : SUSE Linux Enterprise Live Patching 12-SP3 SUSE Linux Enterprise Workstation Extension 15 SUSE Linux Enterprise Module for Legacy Software 15 SUSE Linux Enterprise Module for Development Tools 15	30/08/2018	CVE-2018- 10902	4.18.5 Télécharger	Effectuez une mise à jour du système	10.0

Vulnérabilité dans le Noyau Linux d'UBUNTU	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : Ubuntu 18.04 LTS Ubuntu 16.04 LTS	29/08/2018	CVE-2018- 13406	4.18.5 Télécharger	Effectuez une mise à jour du système	10.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans PHP	Plusieurs vulnérabilités ont été corrigées dans PHP. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'accéder aux informations confidentielles. Les versions affectées sont les suivantes : PHP versions 7.2.x antérieures à 7.2.9	21/08/2018	–	7.2.9 Télécharger	Mettre à jour PHP	8.4
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance.	30/08/2018	CVE-2018-16058	2.6.3 Télécharger	Effectuez une mise à jour de l'application	10.0

Vulnérabilité dans Apache Tomcat Native Connector	Apache a publié des mises à jour de sécurité pour corriger des vulnérabilités dans Apache Tomcat Native Connector. Un attaquant distant pourrait exploiter ces vulnérabilités pour prendre le contrôle d'un serveur affecté. Apache Tomcat Native Connector versions antérieures à 1.2.17	24/08/2018	CVE-2018-8019	1.2.43 Télécharger	Effectuez une mise à jour du connecteur	4.2
Vulnérabilité dans Apache Struts 2	Une vulnérabilité a été corrigée dans Apache Struts 2. Un attaquant distant pourrait exploiter cette vulnérabilité afin de provoquer une exécution de code arbitraire à distance. Les versions vulnérables sont : Struts versions 2.5.x antérieures à 2.5.17	24/06/2018	CVE-2018-11776	2.5.17 Télécharger	Effectuez une mise à jour le framework	8.0
Vulnérabilité dans les produits Adobe Photoshop CC	Une critique vulnérabilité a été corrigée dans Adobe Photoshop CC. Un attaquant pourrait exploiter cette vulnérabilité pour prendre le contrôle d'un système affecté. Les versions vulnérables sont : Photoshop CC 2018 versions antérieures à 19.1.6	24/08/2018	CVE-2018-12811	19.1.6 Contacter Adobe	Effectuez une mise à jour de l'application	6.2

Vulnérabilité dans OpenSSH	Plusieurs vulnérabilités ont été corrigées dans OpenSSH. Un attaquant distant pourrait exploiter ces vulnérabilités afin de provoquer un problème de sécurité non spécifié par l'éditeur. OpenSSH toutes versions antérieures à 7.8	28/08/2018	CVE-2018-15473	7.8 Télécharger	Effectuez une mise à jour	6.2
Vulnérabilité dans les produits Cisco Data Center Network Manager	Cisco a publié une mise à jour de sécurité pour corriger une vulnérabilité dans Cisco Data Center Network Manager. Un attaquant distant pourrait exploiter cette vulnérabilité pour accéder à des informations sensibles. Les systèmes affectés sont les suivants : Cisco Data Center Network Manager (DCNM) versions antérieure à 11.0(1).	29/08/2018	CVE-2018-0464	11.0(1) Contacter Cisco	Veuillez-vous référer au bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180828-dcnm-traversal	8.1

II. ACTUALITÉS

1. Microsoft confirme à moitié l'existence d'une faille 0-day

La faille 0-day mise en lumière par SandboxEscaper permet ce que l'on appelle une escalade de privilège. Pour simplifier, tout utilisateur d'un système étant en capacité d'exécuter du code sur sa machine tournant sur Windows 10 peut acquérir les privilèges administrateur.

https://www.clubic.com/antivirus-securite-informatique/actualite-845127-microsoft-demi-mot-existence-faille-day.html

2. Une chercheuse découvre une faille 0-day dans windows

Habituellement, les chercheurs en sécurité prennent toujours quelques précautions quand il s'agit de publier des failles de sécurité. SandboxEscaper, de son côté, n'y est pas allée par quatre chemins : elle a directement publié sur Twitter et GitHub – et avec un langage fleuri - les preuves d'une vulnérabilité dans la gestion des tâches de Windows. Cette faille permet à un attaquant capable d'exécuter du code sur une machine et d'obtenir les droits systèmes, ce qui est juste en dessous des droits administrateurs.

https://www.01net.com/actualites/cette-chercheuse-decouvre-une-faille-zero-day-dans-windows-10-et-la-publie-sur-twitter-1514198.html

3. Yahoo va éplucher les emails pour revendre les profils à des fins publicitaires

Il y a plus d'un an, Google a annoncé ne plus scanner les emails à des fins publicitaires. Ce qui lui a fait gagner un peu de crédibilité en matière de protection des données personnelles. Chez Yahoo, en revanche, c'est l'inverse. Non seulement le fournisseur continue de scanner les emails de ses utilisateurs, il en fait même un cheval de bataille auprès des annonceurs.

https://www.01net.com/actualites/yahoo-va-eplucher-vos-emails-pour-revendre-votre-profil-a-des-fins-publicitaires-1513720.html

4. Sur Android des commandes secrètes permettent de pirater des millions de smartphones

La prochaine fois que vous voudrez connecter votre smartphone Android à un point de recharge public USB, réfléchissez-y à deux fois. Des chercheurs en sécurité viennent de révéler qu'un grand nombre de modèles peuvent alors être manipulés au travers de commandes spéciales dites « AT ». Parmi les cas les plus graves, les chercheurs ont remarqué qu'il était possible de court-circuiter un écran de verrouillage, de passer des coups de fils, d'envoyer des SMS, de simuler des entrées tactiles ou d'accéder à des données stockées dans la carte SD. Les chercheurs ont publié leurs résultats sur un site web baptisée « ATtention Spanned ».

https://www.01net.com/actualites/android-des-commandes-secretes-permettent-de-pirater-des-millions-de-smartphones-1512460.html

5. L’authentification sans un mot de passe sur le web c’est pour bientôt

Entrez votre identifiant et votre mot de passe … Les habitués des sites Web connaissent la routine et doivent jongler entre une multitude d’identifiants et de sésames. Un vrai casse-tête ! Certes, les navigateurs disposent de fonctions pour enregistrer les mots de passes et il existe des gestionnaires spécialisés tels que KeePass, mais cela est loin de résoudre le problème.

https://www.01net.com/actualites/l-authentification-sans-mot-de-passe-sur-le-web-c-est-pour-bientot-1475642.html

6. Antivirus contre logiciels malveillants : l’histoire d’une lutte sans fin

Les menaces de sécurité et les solutions de protection évoluent sans cesse. Depuis les premiers virus apparus dans les années 70, les vers, chevaux de Troie, botnets ou ransomwares ont transformé ce qui était une simple plaisanterie de hacker en une économie parallèle... Et un challenge continu obligeant les éditeurs de logiciels de sécurité à redoubler d'efforts afin de protéger nos machines.

https://www.clubic.com/antivirus-securite-informatique/logiciel-antivirus/article-844896-1-antivirus-malwares-histoire-poursuite.html

7. La fin du téléphone analogique ?

Vous n'êtes pas sans savoir que la fin des lignes fixes en France s'approche de jour en jour. Les principales craintes émises par la population française semblent tourner autour des zones les moins couvertes par les opérateurs de téléphonie mobile, les zones les moins bien équipées électriquement ou encore, l'isolation des individus n'étant pas familier avec l'outil informatique (notamment les personnes âgées).

https://www.clubic.com/forum/reseaux-wifi-lan/la-fin-de-la-telephonie-analogique-lignes-fixes-pour-ou-contre-id944078-page1.html

III. 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. 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.
4. HIDDEN COBRA - Cyberactivités nord-coréennes malveillantes : Le Département de la Sécurité Intérieure (DHS) et le Bureau Fédéral d'Investigation (FBI) ont identifié des activités malveillantes imputées au groupe dénommé HIDDEN COBRA, et ont fourni des détails techniques sur les outils et l'infrastructure utilisés par ces cyber-acteurs du gouvernement nord-coréen. Le but du partage de cette information est de sensibiliser les responsables des Systèmes d'Information sur la possibilité d'infection, et de réduire l'exposition à cette cyberactivité du gouvernement nord-coréen. Les outils de détection, et des solutions de prévention et d'éradication sont contenues dans les articles contenus dans la page suivante :
   https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
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**.