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 Septembre 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 3
II. VULNÉRABILITÉS PUBLIÉES 4
II.1 NAVIGATEURS 4
Vulnérabilité dans Google Chrome 4
Vulnérabilité dans Firefox 4
II.2 SYSTÈMES D'EXPLOITATION 5
Vulnérabilité dans le Noyau Linux d'Ubuntu 5
Vulnérabilité dans le Noyau Linux de SUSE 5
II.3 AUTRES 6
Vulnérabilité dans les produits VMware Content Locker et AirWatch Agent 6
Vulnérabilité dans les produits Cisco 7
III. ACTUALITÉS 8
IV. NOTES IMPORTANTES 10

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	Plusieurs vulnérabilités ont été corrigées dans Google Chrome. Un attaquant distant pourrait exploiter ces vulnérabilités afin de prendre le contrôle du système affecté. Les versions concernées sont celles antérieures à 69.0.3497.76 pour Windows, Mac et Linux	05/09/2018	CVE-2018- 16069	69.0.3497.76. Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Firefox	Mozilla a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités dans Firefox et Firefox ESR. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour prendre le contrôle d'un système affecté. Mozilla Firefox version antérieure à Firefox 62 ; Mozilla Firefox ESR version antérieure à Firefox ESR 62	06/09/2018	CVE-2018- 12383	62 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 d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un déni de service à distance. Les versions concernées sont les suivantes : Ubuntu 18.04 LTS	11/09/2018	CVE-2018- 13695	4.18.7 Télécharger	Effectuez une mise à jour du système	9.0
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 une élévation de privilèges. Les versions concernées sont les suivantes : SUSE Linux Enterprise Live Patching 15-SP3	11/09/2018	CVE-2018- 10853	4.18.7 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
Vulnérabilité dans les produits VMware Content Locker et AirWatch Agent	De multiples vulnérabilités ont été découvertes dans VMware Content Locker et AirWatch Agent. Elles permettent à un attaquant de provoquer une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les versions vulnérables sont : VMware AirWatch Agent versions antérieures à 5.8.1 sur iOS, et VMware Content Locker versions antérieures à 4.14 sur iOS	05/09/2018	CVE-2018-6976	Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2018-0023.html	6.2

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.	06/09/2018	CVE-2018-0435	Contacter Cisco	Veuillez-vous référer au bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-umbrella-api	9.1

III. Actualités

1. Des failles découvertes dans les VPN populaires

Découvertes par les chercheurs de Cisco Talos, ces deux failles de sécurité concernent les clients NordVPN et ProtonVPN, qui sont deux services très prisés par les utilisateurs. Ces deux brèches permettent aux pirates, via la création d'une ligne de commande OpenVPN, d'exécuter du code malveillant sur les machines Windows.

https://www.clubic.com/antivirus-securite-informatique/vpn/actualite-845336-failles-decouvertes-services-vpn-populaires.html

2. Le pentagone investit dans l'IA

L'Agence pour les projets de recherche avancée de défense (Darpa) va donc bénéficier d'une enveloppe de 2 milliards de dollars sur cinq ans pour financer des projets de recherche dans le domaine de l'intelligence artificielle. L'agence scientifique de l'armée américaine prévoit de lancer de « multiples » projets dans l'année à venir et de mener à bien la vingtaine de projets déjà entamés à l'heure actuelle

https://www.clubic.com/technologies-d-avenir/intelligence-artificielle/actualite-845320-sr-ludo-pentagone-investissement-precedent-ia.html

3. Des applications espionnes dans l'app store

Apple se vante souvent du fait de faire valider les applications entrant au sein de l'App Store par des humains, et non par un processus automatisé comme c'est le cas pour Google et Android. Cependant, bien que la marque à la pomme puisse bien souvent chanter les louanges de ce procédé, il semblerait qu'il ne soit pas sans failles puisque de nombreuses applications disponibles sur son store ont récemment été signalées comme se comportant comme des espions.

https://www.clubic.com/telecharger/actus-logiciels/actualite-845283-alerte-applications-espions-app-store.html

4. Les attaques de crypto-monnaie en hausse

« Les cryptominers sont récents, mais en plein essor. Avec une opportunité de profits élevés et une faible chance d'être découvert ou stoppé, ce malware apparaît comme une valeur refuge pour les cybercriminels » explique l'étude.

https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-845288-attaques-cryptominages-depassent-ransomware.html

5. Une faille zéro dans le navigateur Tor

Voilà qui n'est pas banal. La société Zerodium, dont la spécialité est l'achat et la revente de failles zero-day, vient de livrer gratuitement l'une de ses marchandises. Elle a révélé sur Twitter l'existence d'une faille zero-day dans Tor Browser version 7, permettant de contourner la protection de l'extension NoScript du navigateur. Celle-ci empêche l'exécution de codes actifs sur les pages web visitées, tels que JavaScript, Java, Flash ou Silverlight, améliorant ainsi la protection contre les attaques de type cross-site scripting ou le fingerprinting.

https://www.01net.com/actualites/une-faille-zero-day-dans-le-navigateur-tor-revelee-sur-twitter-1521201.html

6. Les gouvernements anglo-saxons exigent l'installation des backdoors dans les logiciels

Au début, le ton est cordial, mais à la fin il devient beaucoup plus menaçant. Après une réunion la semaine dernière, les agences gouvernementales du groupement « Five Eyes » (Royaume-Uni, Australie, Canada, Nouvelle-Zélande et Etats-Unis) ont publié un communiqué dans lequel ils réclament pour leurs forces de l'ordre un « accès ciblé » aux données chiffrées dans les systèmes et les communications, dans le mesure où « la confidentialité n'est pas absolue ».

https://www.01net.com/actualites/les-gouvernements-anglo-saxons-exigent-l-installation-de-backdoors-dans-nos-logiciels-1517197.html

7. Le hacker de Sony inculpé aux USA

Après plusieurs années d'enquête, les USA auraient mis la main sur le hacker à l'origine - entre autres - de l'attaque des studios Sony. Des poursuites pénales et des sanctions ont été prises contre ce programmeur informatique qui aurait des liens avec les services de renseignements militaires nord-coréens.

https://www.clubic.com/antivirus-securite-informatique/cyberpolice/actualite-845260-sr-cybercrime-hacker-nord-coreen-attaque-sony-inculpe-usa.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. 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**.