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 Mai 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
II.2 SYSTÈMES D'EXPLOITATION 5
Vulnérabilité dans le Noyau Linux de Red Hat 5
Vulnérabilité dans le Noyau Linux de SUSE 5
Vulnérabilité dans le Noyau Linux d'UBUNTU 5
II.3 AUTRES 6
Vulnérabilité dans les routeurs D-Link DIR-620 6
Vulnérabilité dans les produits CISCO 6
Vulnérabilité dans Mozilla Thunderbird 7
Vulnérabilité dans le client DHCP sur RedHat 7
Vulnérabilité dans le Cloud << VMware NSX SD-WAN>> 8
Vulnérabilité dans Git 8
III. ACTUALITÉS 9
IV. NOTES IMPORTANTES 11

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. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les versions affectées sont celles antérieures à 67.0.3396.62 pour Windows, Mac et Linux	30/05/2018	CVE-2018-6147	67.0.3396.62 Télécharger	Mettre à jour le navigateur	9.4

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le Noyau Linux de Red Hat	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.	25/05/2018	CVE-2018- 3639	4.17-rc7 Télécharger	Effectuez une mise à jour du système	8.2
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.	25/05/2018	CVE-2017- 1000199	4.17-rc7 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. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un déni de service. Les systèmes infectés sont les suivants : Ubuntu 17.10 & 16.04 LTS	25/05/2018	CVE-2018-8822	4.17-rc7 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 routeurs D-Link DIR-620	Des chercheurs de Kaspersky Lab ont découvert plusieurs vulnérabilités et un backdoor affectant les routeurs D-Link DIR-620. Le Backdoor consiste en une identification codée en dur « hardcoded » sur l'équipement vulnérable. L'exploitation de ces vulnérabilités ou de ce Backdoor peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire à distance ou d'accéder à des données confidentielles.	24/05/2018	CVE-2018-6213	Contacter D-Link	- Restreindre l'accès à l'interface web en utilisant des whitelists d'adresses IP de confiance. - Restreindre l'accès par Telnet.	5.3
Vulnérabilité dans les produits CISCO	Plusieurs vulnérabilités ont été corrigées dans les produits Cisco. Un attaquant distant pourrait exploiter ces vulnérabilités pour accéder aux informations confidentielles.	22/05/2018	CVE-2018-3640	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	10.0

Vulnérabilité dans Mozilla Thunderbird	Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant de corriger plusieurs vulnérabilités dans le client de messagerie Mozilla Thunderbird. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire à distance, l'accès à des données confidentielles ou le contournement de la politique de sécurité. Les versions affectées sont celles antérieures à la version 52.8	22/05/2018	CVE-2018-5185	52.8 Télécharger	Mettre à jour le client	6.4
Vulnérabilité dans le client DHCP sur RedHat	Redhat annonce la disponibilité d'une mise à jour de sécurité qui permet de corriger une vulnérabilité critique affectant le client DHCP sur Redhat. L'exploitation de cette vulnérabilité peut permettre à un attaquant dans le réseau local d'exécuter des commandes arbitraires avec des privilèges « root ». Les systèmes affectés sont les suivants : Client DHCP sur Red Hat Enterprise Linux Server 6 et 7	16/05/2018	CVE-2018-1111	7.5 (Kernel 3.10.0-862)	Mettre à jour le paquet dhclient	3.0

Vulnérabilité dans le Cloud << VMware NSX SD-WAN>>	Vmware a publié la correction d'une vulnérabilité affectant son produit d'optimisation de trafic dans le Cloud « VMware NSX SD-WAN ». L'exploitation de cette vulnérabilité peut permettre à un attaquant l'exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : VMware NSX SD-WAN Edge by VeloCloud versions antérieures à 3.1.0 sur Linux	16/05/2018	CVE-2018-6961	Contacter VMware	Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs https://my.vmware.com/web/vmware/info?slug=networking_security/vmware_nsx_sd_wan_edge/3_1_1	4.3
Vulnérabilité dans Git	De multiples vulnérabilités ont été découvertes dans Git. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données Git versions 2.17.x antérieures à 2.17.1	29/05/2018	CVE-2018-11235	2.17.1 Télécharger	Mettre à jour le paquet git	6.1

III. ACTUALITÉS

1. Facebook fermera pour un mois en Papouasie Nouvelle Guinée

Une nation de plus de 6 millions de personnes s'apprête à vivre une grande coupure : le gouvernement de Papouasie-Nouvelle-Guinée veut interrompre l'accès à Facebook cette année pendant tout un mois. Une grande « detox numérique » imposée par le ministère des communications et piloté par l'institut national de recherche (National Research Institute).

https://www.01net.com/actualites/facebook-fermera-pour-un-mois-en-papouasie-nouvelle-guinee-1459397.html

2. Une extension sur Chrome qui vous dit si votre mot a été piraté

Les mots de passe que vous utilisez sont-ils réellement sécurisés ? Est-ce qu'ils ne circulent pas déjà parmi les pirates ? La question se pose car, ces dernières années, les identifiants de plusieurs milliards de comptes utilisateurs ont été siphonnés dans des bases de données peu sécurisées pour être revendus sous le manteau, notamment sur le darknet.

https://www.01net.com/actualites/chrome-cette-extension-vous-dit-si-votre-mot-de-passe-a-ete-pirate-1458911.html

3. Le fondateur de Snapchat tacle Facebook et sa manie de copier ses bonnes idées

Le fondateur de Snapchat Evan Spiegel semble condamné à justifier éternellement sa nouvelle version et son design qui ont suscité une bronca impressionnante chez ses utilisateurs. C'est ce qu'il a de nouveau longuement fait lors d'une interview sur scène à la Code Conference. Mais le plus drôle était ailleurs. Interrogé sur la façon dont Facebook a copié les fonctionnalités qui ont fait son succès comme les Stories ou les filtres en réalité augmentée, il a réagi avec beaucoup de sérénité.

https://www.01net.com/actualites/le-fondateur-de-snapchat-tacle-facebook-et-sa-manie-de-copier-ses-bonnes-idees-1459585.html

4. Un pirate vole 18 millions de dollars en prenant le contrôle d'une Blockchain

C'est l'un des pires scénarios qui peut arriver à une cryptomonnaie. Un pirate a réussi à prendre le contrôle de la blockchain de bitcoin gold, une variante du bitcoin créée par la société éponyme, en accaparant plus de 51 % de la puissance de calcul de minage.

https://www.01net.com/actualites/un-pirate-a-vole-18-millions-de-dollars-en-prenant-le-controle-d-une-blockchain-1458134.html

5. Un malware Nord-Coréen sur le google Play store

Le Play Store n'est jamais à l'abri des malwares. Il arrive assez régulièrement que la boutique de Google héberge des applications touchées par un virus ou des logiciels volontairement malveillants. McAfee, spécialiste de la sécurité, a découvert qu'une équipe de développeurs nord-coréens serait à l'origine de trois applis pour le moins problématiques. Celles-ci auraient pour unique but de traquer les déserteurs de la dictature dans le monde entier.

https://www.01net.com/actualites/un-malware-nord-coreen-sur-le-google-play-store-1451174.html

6. Le top 5 des menaces les plus courantes sur mobiles

Les téléphones mobiles sont devenus du fait de leur nombre la cible favorite des cybercriminels. Avast, l'éditeur de solutions de sécurité, a enregistré 5,1 millions d'attaques contre les smartphones entre avril et juin 2017, contre 3,6 millions pour la même période de l'année précédente. Décryptage des menaces.

https://www.01net.com/actualites/securite-sur-mobile-le-top-5-des-menaces-les-plus-courantes-1256646.html

7. Une faille permettant de géolocaliser n'importe quel abonné mobile aux USA

Un nouveau scandale est en train de prendre forme outre-Atlantique autour des services de géolocalisation. Et il risque de faire tache d'huile un peu partout dans le monde. L'histoire commence il y a une semaine, quand le New York Times révèle qu'un shérif utilisait les services payants de Securus Technologies pour géolocaliser une dizaine de personnes via leur téléphone mobile, et cela en dehors de toute autorisation judiciaire. Cette géolocalisation s'appuie sur les antennes-relais avec lesquelles les smartphones sont en connexion permanente dès qu'ils sont allumés.

https://www.01net.com/actualites/une-faille-permettait-de-geolocaliser-n-importe-quel-abonne-mobile-aux-etats-unis-1448819.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**.