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 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.

II. Vulnérabilités publiées

II.1 Système d'exploitation

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Oracle Solaris	Une Vulnérabilité dans le composant Solaris d'Oracle Sun Systems Products Suite, permet à un attaquant à faible privilège avec un accès local, de compromettre le système. L'exploitation de cette vulnérabilité permettrait l'obtention du maximum de privilège et un contrôle total du système à l'attaquant. Les versions vulnérables sont : Solaris version 10 et 11.3.	18/07/2018	CVE-2018-2892	11.3	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	7.2
	Une Vulnérabilité dans le composant Solaris d'Oracle Sun Systems Products Suite, permet un attaquant à faible privilège avec un accès réseau via ISCSI, de compromettre le système. L'exploitation de cette vulnérabilité permettrait un déni de service et une perte de confidentialité des données. Les versions vulnérables sont : Solaris version 11.3.	18/07/2018	CVE-2018-2926			8.0

II.2 SERVEUR WEB

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Oracle weblogic_server	Une vulnérabilité dans le composant Oracle WebLogic Server d'Oracle Fusion Middleware (sous-composant: WLS Core Components), permettrait via le réseau à un attaquant non authentifié de prendre le contrôle du serveur Weblogic. Les versions vulnérables sont : 10.3.6.0, 12.1.3.0, 12.2.1.2 et 12.2.1.3.	18/07/2018	CVE-2018-2893	12c	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	7.5
	Une vulnérabilité dans le composant Oracle WebLogic Server d'Oracle Fusion Middleware (sous-composant: WLS - Web Services), permettrait via le réseau à un attaquant non authentifié via le protocole http, de prendre le contrôle du serveur Weblogic. Les versions vulnérables sont : 10.3.6.0, 12.1.3.0, 12.2.1.2 et 12.2.1.3.	18/07/2018	CVE-2018-2894			7.5

II.3 SGBD

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans MySQL	Une vulnérabilité dans MySQL Server d'Oracle, facilement exploitable permet à un attaquant hautement privilégié ayant un accès réseau via plusieurs protocoles de compromettre le serveur MySQL. Les attaques réussies de cette vulnérabilité peuvent entraîner un déni de service. Les versions affectées sont les suivantes : 5.7.22 et antérieure, 8.0.11	18/07/2018	CVE-2018-3054	Server 8 Télécharger	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	4.0
Vulnérabilités dans Oracle Database Server	Une vulnérabilité dans le composant SGBDR Core d'Oracle Database Server, facilement exploitable permet à un attaquant ayant de faibles privilèges d'ouvrir une session locale avec une connexion à l'infrastructure où le SGBDR Core s'exécute. Bien que la vulnérabilité concerne les SGBDR Core, les attaques peuvent avoir un impact significatif sur d'autres produits. Les versions affectées sont les suivantes : 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1 et 18.2	18/07/2018	CVE-2018-2939	18c INFOS	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	3.6

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Java SE	Une vulnérabilité dans Java DB de Java SE d'Oracle permet à un attaquant non authentifié ayant un accès réseau, via plusieurs protocoles, de compromettre Java SE ainsi que les applications développée en Java s'exécutant sur le système. Les versions affectées sont les suivantes : Java SE: 6u191, 7u181 et 8u172.	18/07/2018	CVE-2018-2938	10.0.2 Télécharger	Veuillez-vous référer au bulletin de sécurité d'Oracle http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	6.8
Vulnérabilité dans Oracle mysql_workbench	Une vulnérabilité dans le composant MySQL Workbench d'Oracle MySQL (dans le module de sécurité chargé du chiffrement) permet à un attaquant non authentifié ayant un accès réseau, via plusieurs protocoles, d'accéder sans autorisation à certaines données. compromettre MySQL Workbench. Les versions affectées sont les suivantes : Oracle Mysql Workbench version 6.3.10 et antérieures.	18/07/2018	CVE-2018-2598	8.0.12 Télécharger	Veuillez-vous référer au bulletin de sécurité d'Oracle http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	4.3

Vulnérabilités dans Oracle vm_virtualbox	Une vulnérabilité dans Oracle VirtualBox permet à un attaquant non authentifié de se connecter au serveur sur lequel il s'exécute et de causer des dénis de service partiels sur celui-ci. Les versions affectées sont les suivantes : Oracle VirtualBox version 5.2.16 et antérieures.	18/07/2018	CVE-2018-3005	5.2.16 Télécharger	Veuillez-vous référer au bulletin de sécurité d'Oracle http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html	2.1

III. ACTUALITÉS

1. **Exobot : un malware qui s'attaque à vos comptes bancaires**

   En ce moment, un nouveau malware baptisé Exobot est en train de se répandre sur les smartphones Android et il a pour particularité de voler vos données bancaires afin de vider vos comptes.
   https://hitek.fr/actualite/malware-exobot-comptes-bancaires-argent-code-source_16833

2. **Malware Glancelove : Espionnage sous couverture lors de la coupe du monde de football**

   Lorsque le coup de sifflet du premier match de la Coupe du Monde 2018 a retenti, cela n'a pas seulement marqué le début d'un tournoi mondialement suivi par les fans de football, cela a également donné le feu vert aux pirates informatiques d'exploiter cet événement à leurs propres fins.
   https://www.globalsecuritymag.fr/Malware-GlanceLove-Espionnage-sous,20180713,79848.html

3. **Infection au rançongiciel SamSam : la plupart des entreprises préfèrent se taire**

   Le ransomware (rançongiciel) SamSam a déjà permis de mettre la main sur quelque 5,9 millions de dollars depuis qu'il s'est manifesté pour la première fois fin 2015 et qu'il a fait pas mal de victimes belges.
   http://datanews.levif.be/ict/actualite/infection-au-rancongiciel-samsam-la-plupart-des-entreprises-preferent-se-taire/article-normal-872925.html

4. **Cisco Talos découvre 20 failles au sein de Samsung Smarttings Hub**

   Dans un post de blog publié le 26 juillet 2018, un chercheur de Cisco Talos explique avoir découvert 20 failles de sécurité au sein de SmartThings Hub, la plateforme dédiée à la maison connectée de Samsung.
   https://www.objetconnecte.com/smartthings-hub-cisco-talos/

5. **HP met à l'épreuve la sécurité de ses imprimantes pour 10.000 dollars**

   Misant beaucoup sur la sécurité de ses appareils, HP n'hésite pas de lancer des défis aux utilisateurs pour en tester l'efficacité. Après l'inscription sur la plateforme Bugcrowd, le testeur disposera d'une quinzaine de modèles d'imprimantes, accessibles à distance. S'il découvre des failles critiques, HP lui octroiera une récompense. Un wiki est déjà mis en place depuis 2017 après la découverte de nombreuses failles sur les imprimantes HP.
   https://itsocial.fr/actualites/hp-met-a-lepreuve-securite-de-imprimantes-10-000-dollars/

6. **Reddit dévoile une faille de sécurité « sérieuse » décoouverte le 19 juin- BGR**

   Reddit a dévoilé un incident de sécurité décrit comme une « attaque sérieuse », sur laquelle il enquête depuis plus d'un mois. Selon la société, un pirate informatique aurait pénétré dans certains de ses systèmes et accédé aux données des utilisateurs. Ces données comprenaient certaines adresses électroniques actuelles, ainsi qu'une ancienne sauvegarde de base de données contenant des mots de passe salés et hachés.
   https://teles-relay.com/reddit-devoile-une-faille-de-securite-serieuse-decouverte-le-19-juin-bgr/

7. **Leure informatique : deux adolescents hameçonnés sur Facebook à Sherbrooke**

   Une enquête criminelle est en cours au Service de police de Sherbrooke, alors que deux adolescents de la région auraient été hameçonnés sur le réseau social Facebook.
   https://ici.radio-canada.ca/nouvelle/1115901/leurre-informatique-adolescents-hameconnes-fortnite-facebook-sherbrooke

8. **Trois hackers ukrainiens arrêtés pour avoir piraté une centaine de société américaines**

   Trois hackers ukrainiens ont été arrêtés aux Etats-Unis pour avoir piraté les systèmes informatiques d'une centaine de sociétés américaines, dérobant les numéros de cartes de crédit de 15 millions de clients, a indiqué mercredi le ministère américain de la Justice.
   http://www.lalibre.be/dernieres-depeches/belga/trois-hackers-ukrainiens-arretes-pour-avoir-pirate-une-centaine-de-societes-americaines-5b62176455326925486f24ca

9. **Le concepteur du rançongiciel qui a paralysé Atlanta serait millionnaire**

   Des chercheurs en sécurité informatique ont découvert que SamSam, le rançongiciel qui a paralysé Atlanta en mars dernier, pourrait avoir rapporté près de 6 millions de dollars américains à son concepteur. Celui-ci agirait seul.
   https://ici.radio-canada.ca/nouvelle/1115904/samsam-rancongiciel-atlanta-ransomware-bitcoin

10. CCleaner : attention, l'application espionne ses utilisateurs à marche forcée

CCleaner espionne ses utilisateurs sans qu'ils ne puissent y échapper : l'application collecte des données présentées comme anonymes, et une option pour désactiver cette télémétrie existe bien. Mais depuis la dernière mise à jour, lorsque l'on désactive la collecte de données, celle-ci se réactive automatiquement. De quoi écorner la réputation de cet utilitaire qui avait déjà été touché par un malware.
http://www.phonandroid.com/ccleaner-espionne-ses-utilisateurs-a-marche-forcee.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**.