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 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 3
II. VULNÉRABILITÉS PUBLIÉES 4
II.1 SGBD 4
Vulnérabilité dans MySQL 4
Vulnérabilités dans Oracle Database Server 5
II.2 AUTRES 6
Vulnérabilité dans les processeurs Intel et ARM 6
Vulnérabilité dans Java SE 7
Vulnérabilité dans FFMPEG 7
Vulnérabilités dans Wireshark 7
III. ACTUALITÉS 8
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 SGBD

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans MySQL	De multiples vulnérabilités ont été découvertes dans Oracle MySQL. 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 déni de service. Les versions affectées : • MySQL Server versions 5.5.60 et antérieures, versions 5.6.40 et antérieures, versions 5.7.22 et antérieures, versions 8.0.11 et antérieures • MySQL Client versions 5.5.60 et antérieures, versions 5.6.40 et antérieures, versions 5.7.22 et antérieures, versions 8.0.11 et antérieures • MySQL Workbench versions 6.3.10 et antérieures, versions 8.0.11 et antérieures • MySQL Connectors versions 5.3.10 et antérieures, versions 8.0.11 et antérieures	18/07/2018	-	Server 8 Télécharger Workbench 6.3 Télécharger	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018verbose-4258253.html#MSQL	9.8

Vulnérabilités dans Oracle Database Server	De multiples vulnérabilités ont été découvertes dans Oracle Database Server. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Versions affectées : Oracle Database Server versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1 et 18.2	17/07/2018	-	18c INFOS	Correctifs disponibles à l'adresse : http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html#AppendixDB	9.8

II.2 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les processeurs Intel et ARM	Les systèmes dotés de microprocesseurs utilisant l'exécution spéculative et la prédiction de branchement peuvent permettre la divulgation non autorisée d'informations à un attaquant avec un accès utilisateur local via un débordement de mémoire spéculatif et une analyse de canal latéral. Ressources affectées : • Processeurs ARM cortex-a ; • Processeurs Intel atom_c, atom_e, atom_x3 et atom_z; • Processeurs Intel celeron_j et celeron_n ; • Processeurs Intel core_i3, core_i5 et core_i7 ; • Processeurs Intel core_m, core_m3, core_m5 et core_m7 ; • Processurs Intel pentium_j et pentium_n ; • Processeurs Intel xeon, xeon_bronze, xeon_e3, xeon_e5, xeon_e7, xeon_gold, xeon_phi, xeon_platinum, et xeon_silver.	10/07/2018	CVE-2018-3693	-	Appliquer les correctifs publiés par les éditeurs de système d'exploitation	4.7

Vulnérabilité dans Java SE	De multiples vulnérabilités ont été découvertes dans Oracle Java SE. 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 déni de service.	21/06/2018	-	10.0.2	Veuillez-vous référer au bulletin de sécurité d'Oracle http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html#AppendixJAVA	10.0
Vulnérabilité dans FFMPEG	Une erreur de traitement des types de trames (différentes de ceux de type EAC3_FRAME_TYPE_INDEPENDENT) ayant plusieurs sous-flux indépendants dans la fonction handle_eac3 dans le fichier libavformat/movenc.c peut déclencher un dépassement d'indice de tableau lors de la conversion d'un fichier AVI spécialement conçu en MPEG4, à un déni de service ou éventuellement à un autre impact non spécifié.	05/07/2018	CVE-2018-13302	4.0.2 Télécharger	Mette à jour en version 4.0.2	6.0
Vulnérabilités dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance. Ressources affectées : Wireshark versions 2.6.0 à 2.6.1, 2.4.0 à 2.4.7 et 2.2.0 à 2.2.15	19/07/2018	CVE-2018-14370	2.6.2 Télécharger	Mettre à jour en version 2.6.2	-

III. ACTUALITÉS

1. **Android : l'UE sanctionne à nouveau Google par une amende record**

   L'UE a sanctionné mercredi Google pour abus de position dominante avec une amende record de 4,34 milliards d'euros, la seconde en un an contre laquelle la firme va faire appel, au risque de détériorer un peu plus les relations entre l'Europe et les Etats-Unis.
   https://information.tv5monde.com/info/android-l-ue-sanctionne-nouveau-google-par-une-amende-record-250420

2. **WhatsApp intègre une option pour faire régner l'ordre dans les discussions de groupe**

   Voilà une décision qui va permettre de mieux s'organiser sur WhatsApp. C'est via un récent billet de blog que la société a annoncé l'arrivée d'une fonctionnalité permettant aux administrateurs d'un groupe d'être les seuls autorisés à poster des messages.
   https://www.journaldugeek.com/2018/07/03/whatsapp-integre-option-faire-regner-lordre-discussions-de-groupe/

3. **Comment pirater un téléphone portable à distance : Guide Complet**

   Vous vous êtes déjà certainement posé la question de savoir Comment pirater un téléphone portable à distance ? Est-il possible d'espionner un téléphone sans y avoir accès ? Ou encore Comment pirater un Android ou iPhone gratuitement ?
   https://www.tutohightech.com/2018/07/pirater-un-telephone-portable-a-distance.html

4. **Patch Tuesday : pluie de fix chez Microsoft, Intel et Adobe**

   Comme chaque mardi, les éditeurs de logiciels. Pas moins de 150 vulnérabilités listées dans la CVE ont ainsi été corrigées chez Adobe, Microsoft et Intel.
   https://www.clubic.com/antivirus-securite-informatique/actualite-844529-patch-tuesday-correctif-failles-vulnerabilites.html

5. **Un hacker tente de vendre des documents classifiés volés à l'US Air Force pour 200 dollars**

   Un pirate informatique a été intercepté alors qu'il tentait de vendre un drone, préalablement volé à l'armée américaine, sur le dark web.
   https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-844515-hacker-vendre-manuel-drone-vole-us-air-force-200-dollars.html

6. **Chine : un malware de minage démasqué, les responsables arrêtés**

   Il n'y a pas un jour sans qu'une affaire criminelle ne fasse la une de la presse crypto. Cette fois-ci, ce sont les autorités chinoises qui ont réussi à mettre la main sur des développeurs de malwares qui ont pu récolter illégalement 2 millions de dollars.
   https://www.barocrypto.com/chine-un-malware-de-minage-demasque-les-responsables-arretes-m316

7. **Microsoft corrige 18 failles critiques en juillet 2018**

   Pour ce mois de juillet, Microsoft a publié 53 correctifs de sécurité dont 18 permettent de combler des failles classées critiques. Notamment celles concernant des vulnérabilités de corruption mémoire dans Edge et le moteur Javascript ChakraCore.
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-corrige-18-failles-critiques-en-juillet-2018-72306.html

8. **L'attaque de logiciels rançonneurs sur la ville d'Atlanta n'était pas aussi grave que nous le pensions... elle était bien pire !**

   Le département de police de la ville a signalé que la plupart de ses preuves vidéo (principalement des vidéos issues de caméras embarquées sur les véhicules de police) ont été perdues. • Plus de 140 applications distinctes ont été totalement ou partiellement neutralisées par l'attaque (près de 30 % des programmes affectés étaient « critiques »)
   http://www.globalsecuritymag.fr/L-attaque-de-logiciels-ranconneurs,20180613,79195.html

9. **Windows 10 : comment supprimer les données de diagnostic**

   Windows 10 collecte beaucoup de données de diagnostic et les envoie à Microsoft. Selon l'éditeur ces données sont anonymes, mais vous souhaitez peut-être savoir ce qui est collecté et surtout comment supprimer ces informations. Cela est désormais possible avec la mise à jour April 2018 Update.
   https://www.01net.com/astuces/windows-10-comment-supprimer-les-donnees-de-diagnostic-1446954.html

10. Un holding d'assurance sud-africain victime d'une cyberattaque

Liberty Holdings, une compagnie d'assurance en Afrique du Sud, a subi samedi une cyberattaque.La société d'assurance a révélé dimanche qu'un hacker qui prétend avoir dérobé des données de l'entreprise réclame de l'argent à leur tour l'économie et la société.
https://www.bbc.com/afrique/region-44512325

11. Le top 5 des métiers du Cloud, du Big data et de la Cybersécurité

En partenariat avec l'Observatoire des métiers des télécommunications (OMT), l'Association pour l'emploi des cadres (Apec) dresse un panorama des métiers et des compétences les plus recherchés dans l'informatique en nuage, les mégadonnées et la sécurité IT.
https://www.silicon.fr/top-5-metiers-cloud-big-data-cybersecurite-214069.html/?inf_by=5b474b1a671db8b65f8b54c4

12. Safe Cyberdefense s'attaque à la sécurité des postes de travail

La jeune pousse française mise en particulier sur des filtres hautement personnalisables pour empêcher l'exécution de codes malicieux. Mais son approche modulaire permet d'aller au-delà avec, notamment, des capacités d'investigation étendues en cas de compromission.
https://www.lemagit.fr/conseil/Safe-Cyberdefense-sattaque-a-la-securite-des-postes-de-travail

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**.