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 Mai 2020

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 Navigateurs

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une exécution de code à distance. Les versions concernées sont les suivantes : • Internet Explorer 11 • Internet Explorer 9	13/05/2020	CVE-2020-1093	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité. Les versions affectées sont : • Firefox versions antérieures à 76 • Firefox ESR versions antérieures à 68.8	05/05/2020	CVE-2020-12396	76 Télécharger	Mettre à jour le navigateur	10.0

Vulnérabilité dans Google Chrome	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire et un déni de service. Les versions affectées sont : Google Chrome versions antérieures à 81.0.4044.138	06/05/2020	CVE-2020-6464	81.0.4044.138 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une usurpation d'identité, une exécution de code à distance et une élévation de privilèges.	13/05/2020	CVE-2020-1197	-	Mettre à jour via Windows Update	9.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 une exécution de code arbitraire et un déni de service. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Server 11-SP4-LTSS • SUSE Linux Enterprise Server 11-EXTRA • SUSE Linux Enterprise Debuginfo 11-SP4	04/05/2020	CVE-2020-9383	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-202014354-1/	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans les produits Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une usurpation d'identité, une exécution de code à distance, un déni de service, un contournement de la fonctionnalité de sécurité et une atteinte à la confidentialité des données.	13/05/2020	CVE-2020-1191	10	Mettre à jour le système via Windows Update	10.0

Vulnérabilité dans le noyau Linux de d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM	04/05/2020	CVE-2020-8649	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/lsn/0066-1/	10.0
Vulnérabilité dans le noyau Linux de Red Hat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et une atteinte à la confidentialité des données.	13/05/2020	CVE-2020-9383	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:2104	10.0
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Google Android toutes versions sans le correctif du 4 mai 2020	04/05/2020	CVE-2020-3645	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2020-05-01	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans WordPress	De multiples vulnérabilités ont été découvertes dans WordPress. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à la confidentialité des données et une injection de code indirecte (XSS). Les versions affectées sont : • WordPress 5.x versions antérieures à 5.4.1, 5.3.3, 5.2.6, 5.1.5, 5.0.9 • WordPress 4.x versions antérieures à 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30 • WordPress 3.x versions antérieures à 3.9.31, 3.8.33, 3.7.33	06/05/2020	-	5.4.1 Télécharger	Mettre à jour le CMS	4.5

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	De multiples vulnérabilités ont été corrigées dans Microsoft .Net. Elles permettent à un attaquant de provoquer un déni de service et une élévation de privilèges.	13/05/2020	CVE-2020-1161		Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans VideoLAN VLC	De multiples vulnérabilités ont été découvertes dans VideoLAN VLC. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un déni de service. Les versions affectées sont les suivantes : • VLC media player versions antérieures à 3.0.9	06/05/2020	CVE-2020-6079	3.0.10 Télécharger VLC	Veuillez-vous référer au Bulletin de sécurité https://www.videolan.org/security/sb-vlc309.html	10.0
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une usurpation d'identité, une atteinte à la confidentialité des données et une exécution de code à distance.	13/05/2020	CVE-2020-1107	2019	Mettre à jour le système via Windows Update	7.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Reader et Acrobat	De multiples vulnérabilités ont été découvertes dans Adobe Reader et Acrobat. 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. Les versions affectées sont les suivantes : • Acrobat DC versions antérieures à 2020.009.20063 sur Windows et macOS • Acrobat Reader DC versions antérieures à 2020.009.20063 sur Windows et macOS • Acrobat 2017 versions antérieures à 2017.011.30171 sur Windows et macOS • Acrobat Reader 2017 versions antérieures à 2017.011.30171 sur Windows et macOS • Acrobat 2015 versions antérieures à 2015.006.30523 sur Windows et macOS • Acrobat Reader 2015 versions antérieures à 2015.006.30523 sur Windows et macOS	13/05/2020	CVE-2020-9615	Télécharger Adobe	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	8.2

Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer un déni de service, une exécution de code à distance et une usurpation d'identité. Les produits affectés sont les suivants : • ChakraCore • Microsoft 365 Apps pour Enterprise pour 64 bits Systems • Microsoft 365 Apps pour Enterprise pour systèmes 32 bits • Microsoft Dynamics 365 (on-premises) version 8.2 • Microsoft Dynamics 365 (on-premises) version 9.0 • Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8) • Microsoft Visual Studio 2019 version 16.0 • Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3) • Microsoft Visual Studio 2019 version 16.5 • Power BI Report Server • Visual Studio Code	13/05/2020	CVE-2020-1192		Effectuez une mise à jour via Windows Update	10.0

III. ACTUALITÉS

1. **The Dark Secrets of a Hacking Hero**
   In may of 2017, Marcus Hutchins saved the internet. A vicious ransomware attack known as WannaCry had infected computer systems across dozens of countries. It was the worst cyberattack in history at the time, and it seemed unstoppable. But Hutchins, a 23-year-old-hacker in Ilfracombe, England, discovered a secret kill switch that stopped the malware from propagating. Hutchins became a celebrity overnight, with the hacker community and the media hailing him as a hero. But all of the newfound attention was not good for him. Three months after defeating the malware, Marcus was arrested by the FBI—not for his involvement in WannaCry, but for a string of past illegal activities that he had kept secret.
   https://www.wired.com/story/gadget-lab-podcast-455/?&web_view=true

2. **The Unattributable "db8151dd" Data Breach**

   I was reticent to write this blog post because it leaves a lot of questions unanswered, questions that we *should* be able to answer. It's about a data breach with almost 90GB of personal information in it across tens of millions of records - including mine. Here's what I know:

   https://www.troyhunt.com/the-unattributable-db8151dd-data-breach/?&web_view=true

3. **Time to change your password!**
   Apple's two-factor authentication (2FA) system for Apple ID accounts deters account hacking by requiring someone both grab your username and password *and* has access to your phone number or a trusted physical device. This alert about a login is an extra check. After correctly entering your user name and password from a new device, a new web browser, a somewhat different geographic location, or even on a previously authenticated device for reasons Apple doesn't disclose, all your associated Apple hardware pops up with the message above, or, if already unlocked or on a Mac, "Apple ID Sign In Requested" with additional information and a small map preview
   https://www.macworld.com/article/3543071/your-iphone-unexpectedly-says-youre-trying-to-log-in-from-far-away-time-to-change-your-password.html?&web_view=true

4. **Microsoft Edge Canary now lets you read aloud your PDF files**
   Microsoft has been working on improvements for Chromium Edge's new cloud-powered Read Aloud feature, which was announced last year. In latest Edge Canary, the company has finally added support for Read Aloud feature in PDFs. If you use Microsoft Edge Canary,

you should be able to add support for Read Aloud feature to PDF files
https://www.bleepingcomputer.com/news/microsoft/microsoft-edge-canary-now-lets-you-read-aloud-your-pdf-files/

5. **L'US Cyber Command expose 3 codes malveillants utilisés par des pirates nord-coréens**

   La Cybersecurity and Infrastructure Security Agency (CISA), le Federal Bureau of Investigation (FBI) et le Department of Defence (DoD) ont publié une alerte de sécurité commune détaillant trois nouvelles variantes de logiciels malveillants utilisées par un présumé groupe de pirates nord-coréens. Un groupe baptisé : Hidden Cobra.

   https://www.zataz.com/lus-cyber-%e2%80%8b%e2%80%8bcommand-expose-3-code-malveillants-utilises-par-des-pirates-nord-coreens/

6. **Industrie 4.0 : De nouveaux vecteurs d'attaques non conventionnels**

   Jusqu'ici, les cyberattaques ayant visé des environnements industriels utilisaient des malwares traditionnels qui pouvaient être contrés par des mécanismes de protection standard du réseau et des postes de travail. Cependant, les hackers sont susceptibles de développer des attaques spécifiques aux technologies opérationnelles (OT) conçues pour passer inaperçues », déclare Nurfedin Zejnulahi, Directeur Technique France chez Trend Micro. « Comme le montrent nos recherches, plusieurs vecteurs sont désormais exposés à ces menaces, ce qui pourrait entraîner des pertes financières et de réputation majeures pour les entreprises de l'Industrie 4.0. Aujourd'hui, la réponse consiste à élaborer une sécurité spécifique à l'OT conçue pour éliminer les menaces sophistiquées et ciblées.
   https://www.undernews.fr/hacking-hacktivisme/industrie-4-0-de-nouveaux-vecteurs-dattaques-non-conventionnels.html

7. **Le malware Ramsay cible les systèmes IT isolés**

   Une étude menée par les chercheurs en sécurité d'Eset montre que plusieurs instances du malware Ramsay sévissent actuellement. Avec un objectif, s'attaquer aux systèmes informatiques isolés et déconnectés des réseaux habituels. Si les systèmes informatiques connectés aux réseaux d'entreprise ou bien publics sont naturellement des ciblent privilégiées des pirates, ceux qui sont déconnectés sont également visés. C'est ce qui ressort d'une dernière recherche d'ESET détaillant le mode opératoire de cyberattaquants utilisant le malware Ramsay. Ce dernier a un objectif aussi simple que clair : identifier, collecter et exfiltrer des données et documents sensibles de systèmes isolés de tout réseau.

   https://www.lemondeinformatique.fr/actualites/lire-le-malware-ramsay-cible-les-systemes-it-isoles-79107.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. Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
4. 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.
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**.