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 d'Avril 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 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. Les versions affectées sont : Google Chrome versions antérieures à 81.0.4044.129	28/04/2020	CVE-2020-6462	81.0.4044.129 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 de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Workstation Extension 15-SP1 • SUSE Linux Enterprise Module for Open Buildservice Development Tools 15-SP1 • SUSE Linux Enterprise Module for Live Patching 15-SP1 • SUSE Linux Enterprise Module for Legacy Software 15-SP1 • SUSE Linux Enterprise Module for Development Tools 15-SP1 • SUSE Linux Enterprise Module for Basesystem 15-SP1 • SUSE Linux Enterprise High Availability 15-SP1	30/04/2020	CVE-2019-11669	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20201141-1/	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 une exécution de code arbitraire, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 19.10 • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM	28/04/2019	CVE-2020-11884	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4346-1/	10.0
Vulnérabilité dans le noyau Linux de Red Hat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.0 ppc64le • Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.0 x86_64	29/04/2020	CVE-2019-19768	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:1966	10.0

Vulnérabilité dans Junos OS	De multiples vulnérabilités ont été découvertes dans Junos OS. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : Juniper Junos OS versions antérieures à 12.3X48-D105, 15.1X49-D220, 15.1R7-S7, 16.1R7-S8, 17.2R3-S4, 17.4R2-S11, 17.3R3-S8, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.3R2-S4, 18.3R3-S2, 18.4R1-S7, 19.1R1-S5, 19.1R3-S1, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2 et 20.1R2 (la date de disponibilité des correctifs n'est pas spécifiée)	27/04/2019	CVE-2020-1631	Contacter Junos OS	Veuillez-vous référer au Bulletin de sécurité https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11021&cat=SIRT_1&actp=LIST	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla !	De multiples vulnérabilités ont été découvertes dans Joomla!. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont : • Joomla! versions antérieures à 3.9.17	22/04/2020	CVE-2020-11891	3.9.18 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 Foxit Reader et PhantomPDF	De multiples vulnérabilités ont été découvertes dans Foxit Reader et PhantomPDF. 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 : • Foxit Reader versions antérieures à 9.7.2 • Foxit PhantomPDF versions antérieures à 9.7.2	24/04/2020	-	Contacter Foxit	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.foxitsoftware.com/support/security-bulletins.php	10.0
Vulnérabilité dans Tenable Nessus	De multiples vulnérabilités ont été découvertes dans Tenable Nessus. Elles permettent à un attaquant de provoquer un déni de service à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Nessus Agent versions antérieures à 7.6.3	29/04/2020	CVE-2020-1967	8.3.1	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.tenable.com/security/tns-2020-03	8.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Zimbra	De multiples vulnérabilités ont été découvertes dans Zimbra. 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 : • Zimbra versions antérieures à 8.8.15 Patch 9	23/04/2020	CVE-2020-1931	8.8.15	Veuillez-vous référer au Bulletin de sécurité https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P9	10.0
Vulnérabilité dans VMware ESXi	Une vulnérabilité a été découverte dans VMware ESXi. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • VMware ESXi versions 6.7.x antérieures à ESXi670-202004103-SG • VMware ESXi versions 6.5.x antérieures à ESXi650-201912104-SG	28/04/2020	CVE-2020-3955	6.7	Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0008.html	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été découvertes dans les produits Microsoft qui utilisent la bibliothèque Autodesk FBX. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance. Les produits affectés sont les suivants : • Microsoft Office 2016 Click-to-Run (C2R) pour éditions 32 bits • Microsoft Office 2016 Click-to-Run (C2R) pour éditions 64 bits • Microsoft Office 2019 pour éditions 32 bits • Microsoft Office 2019 pour éditions 64 bits • Office 365 ProPlus pour systèmes 32 bits • Office 365 ProPlus pour systèmes 64 bits • Paint 3D	21/04/2020	CVE-2020-7085		Effectuez une mise à jour via Windows Update	10.0

III. ACTUALITÉS

1. **28 antivirus exploités pour détruire des fichiers**
   Des chercheurs en sécurité de Rack9 Labs sont parvenus à détourner les fonctions directory junctions et symlinks d'une trentaine d'antivirus du marché pour Windows, Mac et Linux à...
   https://www.lemondeinformatique.fr/actualites/lire-28-antivirus-exploites-pour-detruire-des-fichiers-78900.html

2. **Deux failles zero day dans iOS Mail menacent des milliards d'iPhone et d'iPad**

   Des chercheurs ont découvert deux vulnérabilités de type zero day sur iOS affectant l'application Mail sur les iPhones et iPads. Ces failles, relativement anciennes, sont...

   https://www.lemondeinformatique.fr/actualites/lire-deux-failles-zero-day-dans-ios-mail-menacent-des-milliards-d-iphone-et-d-ipad-78867.html

3. **Des failles zero day découvertes dans IBM Data Risk Manager**

   Un chercheur a découvert quatre failles critiques dans la solution Data Risk Manager d'IBM. Devant le refus de Big Blue de corriger les bugs, il a publié ses travaux. IBM a depuis...

   https://www.lemondeinformatique.fr/actualites/lire-des-failles-zero-day-decouvertes-dans-ibm-data-risk-manager-78852.html

4. **VMware corrige une faille critique dans vCenter Server 6.7**

   Une vulnérabilité de criticité 10 sur l'échelle CVSSv3 a été corrigée en urgence par VMware dans le service d'annuaire vmdir de vCenter Server. Seules certaines versions 6.7 de...

   https://www.lemondeinformatique.fr/actualites/lire-vmware-corrige-une-faille-critique-dans-vcenter-server-67-78767.html

5. **Oracle corrige 405 failles de sécurité sur le trimestre**

   Le bulletin préliminaire du Critical Patch Update trimestriel d'Oracle annonce 405 correctifs à appliquer à 25 familles de logiciels. Un certain nombre de failles sont critiques...

   https://www.lemondeinformatique.fr/actualites/lire-oracle-corrige-405-failles-de-securite-sur-le-trimestre-78758.html

6. **Cyber attaque bancaire à l'encontre de millions de francophones**

   Depuis quelques heures, ZATAZ a repéré une cyber attaque à l'encontre des données privées et personnelles de millions de francophones....

   https://www.zataz.com/cyber-attaque-bancaire-a-lencontre-de-millions-de-francophones/

7. **Fausse alerte virale de votre Windows**

   Un courriel vous indique que votre compte mail est bloqué. Il est conseillé d'utiliser la double authentification. Ne cliquez surtout pas ! On...

   https://www.zataz.com/fausse-alerte-virale-de-votre-windows/

8. **Fuites de données pour l'OMS, Gates Foundation … vraiment ?**

   Des pirates ont diffusé, ce 21 avril, des centaines d'adresses électroniques et mots de passe appartenant à l'Organisation Mondiale de la Santé,...

   https://www.zataz.com/fuites-de-donnees-pour-loms-gates-foundation-vraiment/

9. **Escroquerie aux Bitcoin : vas-y donnes-moi ton wallet !**

   Un pirate a mis en place ce mardi 21 avril une escroquerie dédiée la cryptomonnaie. Dans son action, des dizaines d'accès à un serveur pour...

   https://www.zataz.com/escroquerie-aux-bitcoins-vas-y-donnes-moi-ton-wallet/

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**.