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 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 3
II. VULNÉRABILITÉS PUBLIÉES 4
II.1 NAVIGATEURS 4
Vulnérabilité dans Mozilla Firefox 4
II.2 SYSTÈMES D'EXPLOITATION 5
Vulnérabilité dans Junos Juniper OS 5
Vulnérabilité dans PAN-OS 5
Vulnérabilité dans le noyau Linux de d'Ubuntu 6
Vulnérabilité dans le noyau Linux de Red Hat 6
II.3 AUTRES 7
Vulnérabilité dans les produits VMware 7
Vulnérabilité dans PHP 7
Vulnérabilité dans Zimbra 8
Vulnérabilité dans GitLab 8
Vulnérabilité dans Samba 8
II.4 ACTUALITÉS 9
III. 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 Mozilla Firefox	Une vulnérabilité a été découverte dans Mozilla Firefox. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont : • Firefox versions antérieures à 78.0.2	10/07/2020		78.0.2 Télécharger	Mettre à jour le navigateur	-

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Junos Juniper OS	Juniper annonce la correction de plusieurs vulnérabilités dans le système d'exploitation Junos utilisé dans ses équipements réseaux. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire à distance, de réussir une élévation de privilèges, de contourner la politique de sécurité ou de porter atteinte à l'intégrité de données. Les systèmes affectés sont les suivants : • Junos OS 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4; • Junos OS Evolved 19.2-EVO, 19.3-EVO, 19.4-EVO, 20.1-EVO;	08/07/2020	CVE-2020-1654	Contacter Junos	Veuillez-vous référer au Bulletin de sécurité http://kb.juniper.net/InfoCenter/index?page=content&id=JSA11033	7.5
Vulnérabilité dans PAN-OS	Palo Alto Networks vient de publier de nouvelles vulnérabilités affectant son système d'exploitation PAN-OS. Une de ces vulnérabilités, identifiée par « CVE-2020-2034 » peut permettre à un attaquant distant non authentifié d'exécuter des commandes arbitraires avec des privilèges « root » si la fonctionnalité « GlobalProtect portal » est activée sur une version vulnérable de PAN-OS. L'exploitation des trois autres vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire, de porter atteinte à la confidentialité des données ou de causer un déni de service. Les systèmes affectés sont les suivants :					

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Palo Alto PAN-OS versions 9.1 antérieures à la version 9.1.3 • Palo Alto PAN-OS versions 9.0 antérieures à la version 9.0.9 • Palo Alto PAN-OS versions antérieures à la version 8.1.15					
Vulnérabilité dans le noyau Linux de d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et un contournement de la politique de sécurité. 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	09/07/2020	CVE-2020-13143	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4419-1	6.5
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 un déni de service à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.	08/07/2020	CVE-2020-12888	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:2851	5.3

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions concernées sont les suivantes : • Fusion versions 11.x antérieures à 11.5.5 sur OS X • VMRC pour Mac versions antérieures à 11.2.0 sur OS X • Horizon Client pour Mac versions antérieures à 5.4.3 sur OS X	10/07/2020	CVE-2020-3974	-	Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0017.html	7.8
Vulnérabilité dans PHP	Une vulnérabilité a été découverte dans PHP. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • PHP versions antérieures à 7.2.32 sur Windows • PHP versions antérieures à 7.3.20 sur Windows • PHP versions antérieures à 7.4.8 sur Windows	10/07/2020	CVE-2020-8159	7.4.8 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.php.net/ChangeLog-7.php#7.4.8	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Zimbra	Une vulnérabilité a été découverte dans Zimbra. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Zimbra versions 9.0.0 antérieures à 9.0.0 P4 • Zimbra versions 8.8.15 antérieures à 8.8.15 P11	03/07/2020	CVE-2020-13653	9.0.0 P4 Télécharger	Mettre à jour en version 3.2.5 ou ultérieure https://blog.zimbra.com/2020/07/new-zimbra-patches-9-0-0-patch-4-and-8-8-15-patch-11/	-
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 13.1.3, 13.0.9 et 12.10.14	07/07/2020	CVE-2020-15525	13.1.3	Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/07/06/critical-security-release-gitlab-13-1-3-released/	5.3
Vulnérabilité dans Samba	De multiples vulnérabilités ont été découvertes dans Samba. Elles permettent à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • Samba versions antérieures à 4.5.0	03/07/2020	CVE-2020-10730	4.12.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.samba.org/samba/security/CVE-2020-10730.html	6.5

II.4 ACTUALITÉS

1. **Twitter massivement piraté : plus de 100 000 $ en bitcoin détournés**
   Le réseau social Twitter a connu un piratage coordonné de comptes d'entreprises et de personnalités d'une ampleur inédite. Une attaque par ingénierie sociale a sans doute permis à...
   https://www.lemondeinformatique.fr/actualites/lire-twitter-massivement-pirate-plus-de-100-000-$-en-bitcoin-detournes-79744.html

2. **Trump confirme une cyber attaque à l'encontre d'une entreprise Russe**
   Le Président Américain, Donald Trump, a confirmé une cyber attaque à l'encontre d'une entreprise Russe accusée d'être à l'origine de centaines de fake news.
   https://www.zataz.com/trump-confirme-une-cyber-attaque-a-lencontre-dune-entreprise-russe/

3. **Zoom adresses Vanity URL Zero-Day**
   Un attaquant peut se faire passer pour un employé de l'entreprise, inviter des clients ou des partenaires à des réunions, puis utiliser une conversation d'ingénierie sociale pour extraire des informations sensibles.
   https://threatpost.com/zoom-vanity-url-zero-day/157510/

4. **Un bogue DNS critique ouvre les serveurs Windows au piratage d'infrastructure**
   Microsoft attribue à la faille «wormable» une note de sécurité de 10 - l'avertissement le plus sévère possible.
   https://threatpost.com/critical-dns-bug-windows-servers-infrastructure-takeover/157427/

5. **Un bogue SAP critique permet une prise de contrôle complète du système d'entreprise**
   L'exploitation du bogue peut permettre à un attaquant de lever des informations sensibles, de supprimer des fichiers, d'exécuter du code, de faire du sabotage, etc.
   https://threatpost.com/critical-sap-bug-enterprise-system-takeover/157392/

6. **Les pirates cherchent à voler la recherche sur le vaccin COVID-19**
   L'APT29, liée à la Russie, a jeté son dévolu sur la recherche pharmaceutique dans les pays occidentaux dans une tentative probable de progresser sur un remède contre le coronavirus.
   https://threatpost.com/state-sponsored-hackers-steal-covid-19-vaccine-research/157514/

7. **Comment les Big 9 veulent s'emparer de la vie numérique des utilisateurs**
   Alibaba, Alphabet, Amazon, Apple, Baidu, Facebook, Microsoft, Rakuten et Tencent : 9 géants du web qui veulent s'approprier nos modes de vie numérique à l'échelle mondiale. En s'appuyant sur la 5G, l'intelligence artificielle, l'automatisation et les technologies analytiques, expose un rapport du cabinet TBR.
   https://www.lemondeinformatique.fr/actualites/lire-comment-les-big-9-veulent-s-emparer-de-la-vie-numerique-des-utilisateurs-79598.html

III. 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**.