**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 d'Août 2019

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 systèmes affectés sont :<br>Google Chrome versions antérieures à 76.0.3809.100 | 07/08/2019 | CVE-2019-5868 | 76.0.3809.100<br>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 RedHat | De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants :<br>• Red Hat Enterprise Linux for Real Time 8 x86_64<br>• Red Hat Enterprise Linux for Real Time for NFV 8 x86_64<br>• Red Hat Enterprise Linux for x86_64 8 x86_64<br>• Red Hat Enterprise Linux for IBM z Systems 8 s390x<br>• Red Hat Enterprise Linux for Power, little endian 8 ppc64le<br>• Red Hat Enterprise Linux for ARM 64 8 aarch64<br>• Red Hat CodeReady Linux Builder for x86_64 8 x86_64<br>• Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le | 08/08/2019 | CVE-2019-13272 | 8<br>Ootpa | Veuillez-vous référer au Bulletin de sécurité<br>https://access.redhat.com/errata/RHSA-2019:2411 | 10.0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 un déni de service, un contournement de la politique de sécurité et un autre problème de sécurité non spécifié par l'éditeur. | 08/08/2019 | CVE-2019-13233 | Contacter SUSE | Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20192073-1/ | 10.0 |
| Vulnérabilité dans le noyau Linux de Debian | De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service à distance et une atteinte à la confidentialité des données. La version affectée est la suivante : Debian stable versions antérieures à 4.19.37-5+deb10u2 | 12/08/2019 | CVE-2019-14284 | 10.0.0 Télécharger | Veuillez-vous référer au Bulletin de sécurité https://www.debian.org/security/2019/dsa-4495 | 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 une exécution de code arbitraire à distance, un déni de service à distance, et un autre problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : Google Android toutes versions n'intégrant pas le correctif de sécurité du 05 août 2019 | 06/08/2019 | CVE-2019-11516 | Pie 9.0 Télécharger | Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/pixel/2019-08-01 | 10.0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Vulnérabilité dans Google Chrome OS | De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Google Chrome OS versions antérieures à 76.0.3809.102 (Platform version : 12239.67.0) | 13/08/2019 | | 76.0.3809.102 Télécharger | Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/08/stable-channel-update-for-chrome-os.html | 10.0 |

## II.3 AUTRES

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans les produits Cisco | De multiples vulnérabilités ont été découvertes dans les produits Cisco. 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 | 08/08/2019 | CVE-2019-1934 | - | Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-asa-privescala | 8.8 |
| Vulnérabilité dans les produits Fortinet | Une vulnérabilité a été découverte dans Fortinet FortiOS. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions vulnérables sont : FortiOS versions antérieures à 6.2.1 | 09/08/2019 | CVE-2018-13367 | 6.2.1 Contacter Fortinet | Veuillez-vous référer au bulletin de sécurité https://fortiguard.com/psirt/%20FG-IR-18-173 | 6.2 |
| Vulnérabilité dans IBM WebSphere | De multiples vulnérabilités ont été découvertes dans IBM WebSphere. Elles permettent à un attaquant de provoquer un déni de service à distance et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : IBM Sterling B2B Integrator versions antérieures à 6.0.2.0 | 05/08/2019 | CVE-2019-4046 | 6.0.2.0 Contacter IBM | Veuillez-vous référer au bulletin de sécurité https://www-01.ibm.com/support/docview.wss?uid=ibm10888617 | 3.1 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans produits VMware | De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants :<br>• ESXi versions 6.7 antérieures à ESXi670-201904101-SG<br>• ESXi versions 6.5 antérieures à ESXi650-201903001<br>• Workstation versions 15.x antérieures à 15.0.3<br>• Workstation versions 14.x antérieures à 14.1.6<br>• Fusion versions 11.x antérieures à 11.0.3 sur OSX<br>• Fusion versions 10.x antérieures à 10.1.6 sur OSX | 05/08/2019 | CVE-2019-5684 | Contacter VMware | Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.vmware.com/security/advisories/VMSA-2019-0012.html | 6.3 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans les produits Moxa | De multiples vulnérabilités ont été découvertes dans les produits Moxa. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants :<br>• NPort 5600 versions 3.8 et antérieures<br>• NPort IA5450A versions 1.5 et antérieures | 12/08/2019 | | Contacter Moxa | Veuillez-vous referez au Bulletin de sécurité de l'éditeur https://www.moxa.com/en/support/support/security-advisory/nport-ia5450a-series-serial-device-servers-vulnerability | 10.0 |
| Vulnérabilité dans Cisco 220 Series Smart Switches | De multiples vulnérabilités ont été découvertes dans Cisco 220 Series Smart Switches. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : Cisco 220 Series Smart Switches versions antérieures à 1.1.4.4 | 07/08/2019 | CVE-2019-1913 | Contacter Cisco | Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass | 9.1 |

# III. ACTUALITÉS

## 1. 22 failles de sécurité détectées sur Adobe Photoshop

Adobe a corrigé 22 vulnérabilités critiques dans son application de retouche photo, Adobe Photoshop CC, qui, selon la société, peut permettre l'exécution de code arbitraire. Dans l'ensemble, Adobe a publié des correctifs pour 119 vulnérabilités critiques importantes en août, notamment 25 bogues critiques sur plusieurs plates-formes. La majorité de ces défauts critiques existent dans Adobe Photoshop CC. Deux autres problèmes ont également été résolus dans Creative Cloud Desktop Application et un dans Adobe Experience Manager.

https://threatpost.com/22-critical-flaws-patched-in-adobe-photoshop/147290/

## 2. L'App mycar expose plus de 60.000 voitures

Une application permettant de démarrer sa voiture à distance aurait exposé plus de 60.000 voitures à de potentiels pirates informatiques. Une série de vulnérabilités ont été découvertes par un hacker, lors de la Def Con 2019 de Las Vegas. 'histoire débute en période de Noël. L'ingénieur Jmaxxz (son pseudonyme lui permet de protéger son identité et l'entreprise pour laquelle il travaille), souhaitait faire un cadeau à sa copine, se plaignant du froid ambiant lorsqu'elle reprenait la route à bord de sa voiture. Afin de remédier au problème, Jmaxxz avait souscrit à l'application connectée MyCar, permettant notamment de démarrer son véhicule à distance pour le préchauffer.

https://www.presse-citron.net/cause-app-mycar-60-000-voitures-exposees-pirates-informatiques/

## 3. Apple offre un million $ de récompense pour trouver des failles dans leurs équipements.

Apple a annoncé qu'il renouvelait un programme visant à récompenser les personnes trouvant des failles sur les iPhones et les Mac. Le montant peut désormais aller jusqu'à un million de dollars. Lors d'une conférence Black Hat qui s'est tenue le 8 août à Las Vegas, Apple a effectivement révélé qu'il pourrait offrir jusqu'à un million de dollars aux hackers qui découvrent une faille dans les iPhones ou les Mac. Cela pourrait alors concerner les vulnérabilités exploitées sans aucune intervention ni clic de l'utilisateur de l'iPhone.

https://www.presse-citron.net/apple-offre-un-million-dollars-ceux-reperent-faille-iphone/

## 4. Plus de 40 failles critiques dans les drivers Microsoft

Pour interagir avec les composants matériels auxquels il a accès, le système d'exploitation Windows s'appuie sur une armée de petits logiciels forts pratiques : les drivers ou pilotes informatiques. Malheureusement, ces programmes peuvent également introduire de sérieuses failles de sécurité, comme viennent de le montrer des chercheurs en sécurité de la société Eclypsium, à l'occasion de la conférence DEF CON, qui vient de se dérouler à Las Vegas.

https://www.01net.com/actualites/plus-de-40-drivers-vulnerables-permettent-de-plomber-durablement-les-pc-windows-1747796.html

## 5. Les appareils photos numériques exposés à des ransomwares

Des failles dans le protocole Picture Transfer Protocole permettent de prendre le contrôle à distance d'un Canon EOS 80D et de chiffrer les photos. Un patch est déjà disponible. Un chercheur en sécurité de Check Point Software vient maintenant de le prouver, en créant pour la première fois un ransomware taillé sur mesure pour un reflex numérique, en occurrence pour le Canon EOS D80. Pour infecter l'appareil et chiffrer toutes ses photos, il suffit que le pirate lance un faux réseau Wi-Fi auquel l'utilisateur se connectera, puis d'initier un script Python pour y parvenir. Aucune interaction avec l'utilisateur n'est nécessaire.

https://www.01net.com/actualites/les-reflex-numeriques-peuvent-eux-aussi-attraper-des-ransomwares-1747938.html

## 6. Un hôpital bloqué par un ransomware

Suite à une attaque informatique, les logiciels de l'établissement ne fonctionnent plus. Tout le travail administratif se fait désormais sur papier. De nouveau, un hôpital français tombe dans le piège d'un ransomware. Cette fois, c'est au tour de l'hôpital privé Clairval, situé dans le 9e arrondissement de Marseille, de connaître les affres du rançonnage informatique. L'attaque a eu lieu le 10 août. « Nous nous sommes rendus compte samedi que notre messagerie était plantée et que nos logiciels étaient infectés par un virus », a expliqué le service communication auprès de France 3. L'établissement ne donne aucune précision sur la nature de l'attaque, mais selon France 3, il s'agit bien d'une tentative de rançonnage.

https://www.01net.com/actualites/a-marseille-l-hopital-clairval-bloque-par-un-ransomware-1748901.html

## 7. Facebook écoutait en douce les conversations des utilisateurs de Messenger

Facebook payait ainsi des centaines de sous-traitants pour écouter ces extraits anonymisés et les retranscrire en version texte. Une manière de vérifier si l'intelligence artificielle de l'application de messagerie interprétait de manière appropriée ces conversations.

https://www.01net.com/actualites/facebook-ecoutait-en-douce-les-conversations-des-utilisateurs-de-messenger-1748829.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**.