**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'Août 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 Google Chrome ..... 4
Vulnérabilité dans Mozilla Firefox ..... 4
II.2 SYSTÈMES D'EXPLOITATION ..... 5
Vulnérabilité dans le noyau Linux de d'Ubuntu ..... 5
Vulnérabilité dans le noyau Linux de Red Hat ..... 5
Vulnérabilité dans Microsoft Windows ..... 5
II.3 CMS ..... 6
Vulnérabilité dans Joomla ..... 6
II.4 AUTRES ..... 7
Vulnérabilité dans GitLab ..... 7
Vulnérabilité dans Mozilla Thunderbird ..... 7
Vulnérabilité dans les produits VMware ..... 8
Vulnérabilité dans BIND ..... 8
Vulnérabilité dans les produits Microsoft ..... 8
Vulnérabilité dans Tenable Nessus ..... 9
Vulnérabilité dans les produits cisco ..... 9
III. ACTUALITÉS ..... 10
IV. NOTES IMPORTANTES ..... 12

# 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 :<br>Google Chrome versions antérieures à 85.0.4183.83 | 26/08/2020 | CVE-2020-6571 | 85.0.4183.83<br>Télécharger | Mettre à jour le navigateur | - |
| 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 à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les versions affectées sont :<br>• Firefox versions antérieures à 80<br>• Firefox ESR versions antérieures à 68.12<br>• Firefox ESR versions 7x antérieures à 78.2 | 26/08/2020 | CVE-2020-15670 | 80<br>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 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 à distance. Les systèmes affectés sont les suivants :<br>• Ubuntu 18.04 LTS | 21/08/2020 | CVE-2020-15393 | 20.04<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4465-1 | 5.5 |
| 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 exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges. | 31/08/2020 | CVE-2019-14896 | 8.2.0<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:3548 | 9.8 |
| Vulnérabilité dans Microsoft Windows | De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants :<br>• Windows 8.1<br>• Windows Server 2012 R2 | 21/08/2020 | CVE-2020-1537 | 10 | Mettre à jour le système via Windows Update | 7.8 |

## 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 et une injection de code indirecte à distance (XSS). Les versions affectées sont :<br><br>• Joomla! versions antérieures à 3.9.21 | 26/08/2020 | CVE-2020-24599 | 3.9.21<br>Télécharger | Mettre à jour le CMS | 6.1 |

## II.4 AUTRES

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| 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 13.2.6, 13.1.8 et 13.0.14 | 20/08/2020 | - | 13.2.6 | Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/08/18/critical-security-release-gitlab-13-2-6-released/ | - |
| Vulnérabilité dans Mozilla Thunderbird | De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une élévation de privilèges. Les versions concernées sont les suivantes :<br>• Thunderbird versions antérieures à 68.12<br>• Thunderbird versions 7x antérieures à 78.2 | 27/08/2020 | CVE-2020-15670 | 78.2 Télécharger | Veuillez-vous référer au Bulletin de sécurité https://www.mozilla.org/en-US/security/advisories/mfsa2020-40/ | - |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans les produits VMware | De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer un déni de service à distance et une injection de code indirecte à distance (XSS). | 20/08/2020 | CVE-2020-3976 | - | Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0019.html | 5.3 |
| Vulnérabilité dans BIND | De multiples vulnérabilités ont été découvertes dans BIND. Elles permettent à un attaquant de provoquer un déni de service à distance. Les systèmes infectés sont les suivants :<br>• BIND versions antérieures à 9.11.22<br>• BIND versions 9.12.x à 9.16.x antérieures à 9.16.6<br>• BIND versions 9.17.x antérieures à 9.17.4 | 21/08/2020 | CVE-2020-8624 | 9.17.4 Télécharger | Veuillez-vous référer au Bulletin de sécurité https://kb.isc.org/docs/cve-2020-8624 | 4.3 |
| 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 atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité | 21/08/2020 | CVE-2020-1591 | - | Mettre à jour le système via Windows Update | 5.4 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans Tenable Nessus | Une vulnérabilité a été découverte dans Tenable Nessus. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes :<br>Nessus versions antérieures à 8.11.1 | 21/08/2020 | CVE-2020-5774 | 8.11.1 | Veuillez-vous référer au Bulletin de sécurité https://www.tenable.com/security/tns-2020-06 | 7.1 |
| Vulnérabilité dans les produits cisco | De multiples vulnérabilités ont été découvertes dans les produits Cisco. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges. | 27/08/2020 | CVE-2020-3517 | | Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxosbgp-nlri-dos-458rG2OQ | 8.6 |

# III. ACTUALITÉS

1. **Microsoft dévoile des outils pour lutter contre les deepfakes**
   Les usurpations et tromperies consistant à manipuler grâce à l'intelligence artificielle des images aussi bien que des flux audio ou video posent de gros soucis. Pour contrecarrer l'essor des deepfakes, Microsoft a dévoilé plusieurs outils dont Video Authenticator et rejoint plusieurs initiatives dont l'AI Foundation.
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-devoile-des-outils-pour-lutter-contre-les-deepfakes-80240.html

2. **La durée de vie des certificats TLS/SSL réduite à 13 mois**
   Le 1er septembre marque des changements importants dans la durée de validité des certificats TLS et SSL. Au lieu de 2 ans, ils seront valables pendant 13 mois.
   https://www.lemondeinformatique.fr/actualites/lire-la-duree-de-vie-des-certificats-tls-ssl-reduite-a-13-mois-80221.html

3. **La moitié des antivirus peinent à détecter les menaces**
   Selon un rapport de l'entreprise de tests SE-Labs, les antivirus disponibles sur le marché ne parviennent pas tous à détecter la plupart des attaques. Les solutions proposées par Kaspersky, Microsoft et McAfee ont été jugées les plus performantes.
   https://www.lemondeinformatique.fr/actualites/lire-la-moitie-des-antivirus-peinent-a-detecter-les-menaces-80068.html

4. **SANS Institute tire les leçons de son piratage**
   Organisme de formation, SANS Institute a joué la transparence sur son piratage. Dans une vidéo, il explique la méthode qui a été utilisée et comment s'en prémunir. Il ne faut jamais manquer une occasion d'apprendre.
   https://www.lemondeinformatique.fr/actualites/lire-sans-institute-tire-les-lecons-de-son-piratage-80085.html

5. **Le gouvernement Canadien ferme plusieurs sites à la suite d'une cyberattaque**
   Peur numérique au Canada. Le gouvernement contraint de fermer la plupart de ses portails administratifs en ligne après une cyberattaque. Chinois, Nord Coréens, Russes ? Newfie, il s'agit peut-être de votre petit cousin. Explication.

   https://www.zataz.com/le-gouvernement-canadien-ferme-plusieurs-sites-a-la-suite-dune-cyberattaque/

6. **Six nouvelles applications du Google Play infectées par le malware Joker**
   Identification de six nouvelles applications proposées sur le Google Play piégées par le malware Joker, un code malveillant qui vous abonne à des services payants.
   https://www.zataz.com/six-nouvelles-applications-du-google-play-infectees-par-le-malware-joker/

7. **Nouveau malware de type Botnet P2P sans fichier ciblant les serveurs SSH du monde entier**
   Des chercheurs en cybersécurité ont dévoilé aujourd'hui un botnet P2P (peer-to-peer) sophistiqué et multifonctionnel écrit en Golang qui cible activement les serveurs SSH depuis janvier 2020.
   https://www.undernews.fr/malwares-virus-antivirus/nouveau-malware-de-type-botnet-p2p-sans-fichier-ciblant-les-serveurs-ssh-du-monde-entier.html

8. **La panne de Centurylink a provoqué une chute de 3,5 % du trafic internet mondial**
   La panne technique essuyée par le FAI américain CenturyLink a conduit à une baisse de 3,5 % du trafic internet mondial. Retour sur l'une des plus grosses coupures d'Internet jamais enregistrées.
   https://www.zdnet.fr/actualites/la-panne-de-centurylink-a-provoque-une-chute-de-35-du-trafic-internet-mondial-39908783.htm

9. **Quel est le plus dangereux store d'applications sur mobile ?**
   Contrairement à ce qu'on pourrait penser, ce n'est pas le Play Store de Google ! Une étude a analysé les risques que chaque plateforme d'achat d'applications représente.
   https://www.zdnet.fr/actualites/quel-est-le-plus-dangereux-store-d-applications-sur-mobile-39899885.htm

10. **Nouvelle activité malveillante du groupe nord-coréen Lazarus (Trojan BLINDINGCAN)**
    Des chercheurs en cybersécurité en association avec le département américain de la sécurité intérieure (DHS) ont découvert un nouveau cheval de Troie d'accès à distance baptisé BLINDINGCAN utilisé par le groupe Lazarus très fortement lié à la Corée du Nord.
    https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

# 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**.