**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 Novembre 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 :<br>Google Chrome versions antérieures à 86.0.4240.198 | 12/11/2020 | CVE-2020-16017 | 86.0.4240.198<br>Télécharger | Mettre à jour le navigateur | - |
| 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 affectées sont les suivantes :<br>• Internet Explorer 11 | 12/11/2020 | CVE-2020-17058 | IE 11<br>Télécharger | Mettre à jour le système via Windows Update | 7.5 |
| Vulnérabilité dans Microsoft Edge | De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une exécution de code à distance. La version affectée est la suivante :<br>• Microsoft Edge (EdgeHTML-based) | 12/11/2020 | CVE-2020-17058 | 86.0.622.51 | Mettre à jour le système via Windows Update | 7.5 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Vulnérabilité dans Mozilla Firefox | Une vulnérabilité a été découverte dans Mozilla Firefox et Thundebird. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance Les versions affectées sont les suivantes :<br>• Firefox versions antérieures à 82.0.3<br>• Firefox ESR versions antérieures à 78.4.1<br>• Thunderbird versions antérieures à 78.4.2 | 10/11/2020 | CVE-2020-26950 | 82.0.3<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 Microsoft Windows | De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une exécution de code à distance, un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, un déni de service et une usurpation d'identité. | 12/11/2020 | CVE-2020-17090 | 10 | Mettre à jour le système via Windows Update | - |
| 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 atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes affectés sont les suivants :<br>• Ubuntu 20.10 LTS<br>• Ubuntu 20.04 LTS<br>• Ubuntu 18.04 LTS<br>• Ubuntu 16.04 LTS<br>• Ubuntu 14.04 ESM<br>• Ubuntu 12.04 ESM | 13/11/2020 | CVE-2020-27194 | 20.04.1<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4627-1 | 5.5 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| 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 problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à l'intégrité des données. | 13/11/2020 | CVE-2020-26950 | 8.3.0<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:5104 | - |
| Vulnérabilité dans Palo Alto PAN-OS | De multiples vulnérabilités ont été découvertes dans Palo Alto PAN-OS. 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 la confidentialité des données. Les versions affectées sont les suivantes :<br>• Palo Alto PAN-OS versions 10.0.x antérieures à 10.0.1<br>• Palo Alto PAN-OS versions 9.1.x antérieures à 9.1.5<br>• Palo Alto PAN-OS versions 9.0.x antérieures à 9.0.11<br>• Palo Alto PAN-OS versions 8.1.x antérieures à 8.1.17 | 12/11/2020 | CVE-2020-2050 | 10.0.1 | Veuillez-vous référer au Bulletin de sécurité https://security.paloaltonetworks.com/CVE-2020-2050 | - |

| 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 noyaux linux de SUSE. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à la confidentialité des données. | 13/11/2020 | CVE-2020-27675 | 15 | Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20203281-1/ | 4.7 |
| Vulnérabilité dans Google Chrome OS | De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants :<br>• Google Chrome OS versions antérieures à 86.0.4240.198 | 13/11/2020 | - | OS86 | Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-chrome-os_12.html | - |

## II.3 AUTRES

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Multiples vulnérabilités dans les produits Apple | De multiples vulnérabilités ont été découvertes dans les produits Apple. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les produits affectés sont les suivants :<br>• Safari versions antérieures à 14.0.1<br>• macOS Big Sur versions 11.0.x versions antérieures à 11.0.1<br>• macOS High Sierra versions 10.13.x versions antérieures à 10.13.6<br>• macOS Mojave versions 10.14.x versions antérieures à 10.14.6 | 13/11/2020 | - | - | Veuillez-vous référer aux Bulletins de sécurité https://support.apple.com/fr-fr/HT211946<br><br>https://support.apple.com/fr-fr/HT211934<br><br>https://support.apple.com/fr-fr/HT211931 | - |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Multiples vulnérabilités dans Nagios XI | De multiples vulnérabilités ont été découvertes dans Nagios XI. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une injection de code indirecte à distance (XSS).<br>Les versions affectées sont les suivantes :<br>Nagios XI versions antérieures à 5.7.5 | 13/11/2020 | - | 5.7.5 | Veuillez-vous référer au Bulletin de sécurité https://www.nagios.com/downloads/nagios-xi/change-log/ | - |
| Multiples vulnérabilités dans Microsoft Office | De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une exécution de code à distance, un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données et une usurpation d'identité. | 13/11/2020 | - | 365 | Effectuer une mise à jour le système via Windows Update | - |
| Vulnérabilité dans Apache OpenOffice | Une vulnérabilité a été découverte dans Apache OpenOffice. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité.<br>Les versions affectées sont les suivantes :<br>OpenOffice versions antérieures à 4.1.7 | 12/11/2020 | CVE-2020-13958 | 4.1.18<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://www.openoffice.org/security/cves/CVE-2020-13958.html | - |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Multiples vulnérabilités dans PostgreSQL | De multiples vulnérabilités ont été découvertes dans PostgreSQL. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un contournement de la politique de sécurité.<br>Les versions affectées sont les suivantes :<br>• PostgreSQL versions 13.x antérieures à 13.1<br>• PostgreSQL versions 12.x antérieures à 12.5<br>• PostgreSQL versions 11.x antérieures à 11.10<br>• PostgreSQL versions 10.x antérieures à 10.15<br>• PostgreSQL versions 9.6.x antérieures à 9.6.20<br>• PostgreSQL versions 9.5.x antérieures à 9.5.24 | 13/11/2020 | CVE-2020-25695<br>CVE-2020-25694<br>CVE-2020-25696 | 13<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité https://www.postgresql.org/about/news/postgresql-131-125-1110-1015-9620-and-9524-released-2111/ | - |
| Multiples vulnérabilités dans Asterisk | De multiples vulnérabilités ont été corrigées dans Asterisk. Elles permettent à un attaquant de provoquer un déni de service et un contournement de la politique de sécurité. | 09/11/2020 | CVE-2020-28327 | 18.0.1<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité ; http://downloads.asterisk.org/pub/security/AST-2020-001.html | - |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| Multiples vulnérabilités dans Intel AMT, ISM et Wireless Bluetooth | De multiples vulnérabilités ont été découvertes dans Intel AMT, ISM et Wireless Bluetooth. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les versions infectées sont les suivantes :<br>• Intel Active Management Technology (AMT) et Intel Standard Manageability (ISM) versions antérieures à 11.8.80, 11.12.80, 11.22.80, 12.0.70 et 14.0.45 (pour la vulnérabilité critique CVE-2020-8752)<br>• Intel CSME et Intel AMT versions antérieures à 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 et 14.5.25<br>• Intel TXE versions antérieures à 3.1.80 et 4.0.30<br>• Intel Server Platform Services versions antérieures à SPS_E5_04.01.04.400, SPS_E3_05.01.04.200, SPS_E3_04.01.04.200, SPS_SoC-X_04.00.04.200 et SPS_SoC-A_04.00.04.300<br>• Intel Wireless Bluetooth versions antérieures à 21.110 | 12/11/2020 | - | - | Veuillez-vous référer aux Bulletins de sécurité<br><br>https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00391.html<br><br>https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00403.html | - |

# III. ACTUALITÉS

1. **Google détaille une faille zero day Windows exploitée**
   Les équipes de chercheurs en sécurité project Zero de Google ont publié les détails concernant la vulnérabilité CVE-2020-117087 actuellement exploitée frappant les systèmes Windows dont la version 7 et 10. Un correctif n'est pas attendu avant 8 jours.
   https://www.lemondeinformatique.fr/actualites/lire-google-detaille-une-faille-zero-day-windows-exploitee-80890.html

2. **Les entreprises en danger selon les RSSI**
   Une étude menée par Bitdefender montre que les RSSI craignent une montée en puissance du risque cyber dans les entreprises. Avec dans le viseur en particulier des ransomwares de plus en plus destructeurs.
   https://www.lemondeinformatique.fr/actualites/lire-les-entreprises-en-danger-selon-les-rssi-80930.html

3. **Le ransomware NewRegret chiffre les machines virtuelles Windows**
   Découvert fin octobre 2020, le rançongiciel RegretLocker utilise une technique originale pour chiffrer des machines virtuelles Windows et leurs contenus.
   https://www.lemondeinformatique.fr/actualites/lire-le-ransomware-newregret-chiffre-les-machines-virtuelles-windows-80938.html

4. **Zero Trust : le choix nécessaire à l'heure du télétravail généralisé**
   Selon une étude réalisée pour Gigamon, la plupart des RSSI et DSI ont adopté l'approche Zero Trust ou prévoient de le faire.
   https://www.lemondeinformatique.fr/actualites/lire-zero-trust-le-choix-necessaire-a-l-heure-du-teletravail-generalise-80965.html

5. **Une nouvelle faille DNS permet d'usurper l'identité de n'importe quel site**
   Des chercheurs ont trouvé un canal auxiliaire qui remet au goût du jour ce type d'attaque que l'on croyait éliminée depuis douze ans.
   https://www.01net.com/actualites/une-nouvelle-faille-dns-permet-d-usurper-l-identite-de-n-importe-quel-site-2005844.html

6. **En 2021, les vieux smartphones Android ne pourront plus se connecter à certains sites Web**
   La société de sécurité Let's Encrypt va commencer à cesser son partenariat de signatures croisées en 2021, ce qui va bloquer l'accès aux sites Web qui utilisent le certificat ISRG Root X1.
   https://www.01net.com/actualites/en-2021-les-vieux-smartphones-android-ne-pourront-plus-se-connecter-a-certains-sites-web-2003957.html

7. **Apple colmate trois failles zero-day critiques exploitées par des pirates**
   Découvertes par Google Project Zero, ces trois failles affectent presque tous les systèmes d'Apple. Elles permettent d'exécuter du code arbitraire à distance, et notamment dans le noyau.
   https://www.01net.com/actualites/apple-colmate-trois-failles-zero-day-critiques-exploitees-par-des-pirates-2002997.html

8. **Chrome : deux failles zero-day exploitées par des pirates corrigées en urgence**
   La série de failles zero-day continue. Il est vivement recommandé de mettre à jour Chrome Desktop et Chrome Android.
   https://www.01net.com/actualites/chrome-deux-failles-zero-day-exploitees-par-des-pirates-corrigees-en-urgence-2001768.html

9. **RegretLocker : ce ransomware s'en prend aussi aux disques virtuels**
   Des chercheurs attirent l'attention sur RegretLocker, ransomware capable de chiffrer des fichiers sur les disques durs virtuels au format Hyper-V.
   https://www.silicon.fr/regretlocker-ransomware-disques-virtuels-350625.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**.