CyberWatch

Veille Cybersécurité Hebdomadaire

ÉDITION S17 — 20 - 26 AVRIL 2026

Systèmes embarqués & IoT | Réglementation cyber CRA / RED / ETSI

4 SIGNAUX CRITIQUES	**3** JALONS RÉGLEMENTAIRES	**2** FOCUS AFRIQUE

Abdoul Karim Mamani Malam Goga

Cybersécurité IoT & Radio | Gouvernance & Conformité CRA / RED / ETSI

 # SOMMAIRE

Contenu de cette édition

VEILLE EMBARQUÉE & IOT

Signaux critiques — 1 & 2

SIGNAL 01 — CVE CRITIQUE

CVE-2026-5194 — wolfSSL | CVSS 9.3 / 10.0

CVE CRITIQUE

Faille critique dans wolfSSL : la vérification des signatures de certificats ne valide pas correctement les digest et OID, permettant à un attaquant de présenter un certificat frauduleux. Conséquences : interception de trafic chiffré (MitM), accès non autorisé à des systèmes sensibles, ou injection de mises à jour malveillantes via le mécanisme OTA.

~5 milliards de dispositifs affectés. Patch : wolfSSL v5.9.1 (8 avril 2026). Équipements anciens ou non maintenus restent exposés.

SIGNAL 02 — CVE CRITIQUE

CVE-2026-32746 — GNU Inetutils telnetd | CVSS 9.8

CVE CRITIQUE

Dépassement de tampon dans le handler LINEMODE SLC du démon telnetd : un attaquant distant non authentifié peut déclencher une exécution de code arbitraire avec privilèges root, sans interaction utilisateur, dès la phase de négociation initiale (TCP/23).

Toutes versions GNU InetUtils jusqu'à 2.7. Très présent dans les environnements ICS/OT et réseaux gouvernementaux africains.

 # VEILLE EMBARQUÉE & IOT

Signal critique 3 & Focus Afrique

SIGNAL 03 — SYSTÈMES EMBARQUÉS

CVE-2026-41503 — BACnet Stack | Divulgué le 24/04/2026

EMBARQUÉ

Lecture hors limites dans le service ReadPropertyMultiple de BACnet Stack (versions antérieures à 1.4.3) : un attaquant peut provoquer un crash ou extraire des données mémoire sensibles. Systèmes exposés : automates de gestion technique du bâtiment (BMS/GTB) et équipements domotiques industriels communicant via BACnet.

Correction : BACnet Stack v1.4.3. Surface d'attaque large dans les bâtiments intelligents intégrant des contrôleurs BACnet non patchés.

🌍 FOCUS AFRIQUE — VEILLE EMBARQUÉE

CVE-2026-5194 représente un risque systémique pour la région : wolfSSL est omniprésente dans les équipements IoT importés sans audit de sécurité préalable, et ces équipements ne reçoivent pratiquement jamais de mises à jour après déploiement. CVE-2026-32746 aggrave ce tableau — Telnet reste activement exposé sur des équipements gouvernementaux et réseau critiques, offrant une surface d'exécution de code à distance sans authentification difficile à contenir dans des environnements à faibles ressources opérationnelles.

VEILLE RÉGLEMENTAIRE

Jalons CRA & ETSI

JALON 01 — CRA

CRA

Jalon CRA : 11 septembre 2026 — Reporting obligatoire des vulnérabilités

À compter du 11 septembre 2026, dans le cadre du Cyber Resilience Act (règlement UE 2024/2847), tout fabricant souhaitant mettre des produits sur le marché européen devra notifier les vulnérabilités activement exploitées selon un calendrier strict : alerte initiale sous 24h, rapport technique détaillé sous 72h, rapport final sous 14 jours. Le cadre d'évaluation par organismes tiers (Notified Bodies) entrera en vigueur le 11 juin 2026 — soit dans moins de 7 semaines.. Non-conformité : jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial.

JALON 02 — ETSI

ETSI

Normes verticales ETSI — 18 catégories en consultation publique

L'ETSI a mis en consultation publique des projets de normes européennes harmonisées couvrant 18 catégories de produits — dont routeurs, systèmes domotiques, caméras de sécurité, verrous connectés, VPN, SIEM et PKI. Publication attendue en octobre 2026 ; documents disponibles librement sur l'ETSI Open Area. Une fois harmonisées et publiées au Journal Officiel de l'UE, ces normes confèreront une présomption de conformité au CRA pour les fabricants ciblant le marché européen.

 # VEILLE RÉGLEMENTAIRE

Jalon NIS2 & Focus Afrique

JALON 03 — NIS2 / RED

NIS2

NIS2 : entrée en supervision active au 18 avril 2026

Depuis le 18 avril 2026, dans les États membres de l'Union Européenne, les autorités nationales compétentes exercent un pouvoir de supervision et de sanction effectif sur les entités relevant de NIS2. Parallèlement, les exigences cybersécurité de la directive européenne RED (articles 3.3 d, e et f) sont opposables depuis août 2025 — or la majorité des importateurs d'équipements radioélectriques n'ont pas encore intégré ces obligations dans leurs processus de mise sur le marché européen.

📋 FOCUS AFRIQUE — RÉGLEMENTAIRE

L'alignement des cadres africains d'homologation sur le CRA et les normes ETSI n'est pas une obligation légale directe — ces textes sont des réglementations de l'Union Européenne qui ne s'appliquent pas au marché africain. Toutefois, les jalons 2026 créent une pression indirecte forte : tout équipement exporté vers l'Europe ou fabriqué par un acteur visant le marché UE devra les respecter. Par ailleurs, la directive RED est déjà opposable depuis août 2025 pour tout équipement radioélectrique mis sur le marché européen — les régulateurs africains qui s'en inspirent pour leurs cadres d'homologation y trouvent un référentiel technique solide et reconnu internationalement.

 # SYNTHÈSE OPÉRATIONNELLE

Recommandations — Immédiat & Court terme

IMMÉDIAT
< 72h

wolfSSL — CVE-2026-5194

Déployer immédiatement wolfSSL v5.9.1 sur l'ensemble des équipements concernés. Constituer un inventaire exhaustif des actifs intégrant wolfSSL — les équipements en fin de vie ou non maintenables doivent être isolés sur un VLAN dédié avec surveillance réseau renforcée. Engager sans délai les fournisseurs pour obtenir une confirmation de correctif ou, à défaut, un plan de remplacement chiffré.

COURT
< 2 semaines

GNU Inetutils telnetd — CVE-2026-32746

Désactiver Telnet (TCP/23) en priorité sur tous les équipements où ce service n'est pas strictement requis par l'exploitation, et le remplacer par SSH lorsque l'infrastructure le permet. Appliquer les correctifs GNU InetUtils disponibles sur les systèmes maintenus. Réaliser un audit d'exposition TCP/23 couvrant l'ensemble du parc ICS/OT, des équipements réseau et des terminaux gouvernementaux — toute interface Telnet exposée sans patch doit être considérée comme compromise.

MOYEN
1 mois

BACnet Stack — CVE-2026-41503

Déployer BACnet Stack v1.4.3 sur l'ensemble des contrôleurs et automates de bâtiment concernés. Segmenter immédiatement les réseaux BMS/GTB sur des VLAN dédiés, isolés du reste du système d'information. Conduire un audit d'inventaire ciblant les équipements tournant sur des versions antérieures à 1.4.3 et établir un plan de mise à jour priorisé par criticité. Intégrer l'ensemble des contrôleurs BACnet au SBOM de l'infrastructure pour assurer leur traçabilité et faciliter les futures opérations de remédiation.

 # SYNTHÈSE OPÉRATIONNELLE

Recommandations stratégiques & Sources

STRAT. Juin 2026

CRA — Notified Bodies applicables le 11 juin 2026

S'assurer que les organismes d'évaluation de la conformité sollicités seront bien notifiés auprès des autorités compétentes d'ici le 11 juin 2026 — soit dans moins de 7 semaines — toute procédure engagée après cette date sera juridiquement invalide. Cartographier les produits relevant de l'évaluation tierce obligatoire (Annexe VIII du CRA) et initier sans délai les procédures correspondantes. Constituer le dossier technique complet : nomenclature des composants (SBOM), déclaration UE de conformité et rapport d'évaluation de sécurité — ces trois documents sont exigibles à la mise sur le marché européen.

STRAT. Sept. 2026

CRA — Reporting vulnérabilités obligatoire le 11 septembre 2026

Mettre en place et tester avant le 11 septembre 2026 la chaîne complète de notification des vulnérabilités activement exploitées : alerte initiale sous 24h, rapport technique détaillé sous 72h, rapport final sous 14 jours. Identifier formellement le CSIRT national compétent pour votre secteur d'activité et établir un canal de communication opérationnel avec lui. Formaliser l'ensemble de ces procédures dans une politique de gestion des vulnérabilités (vulnerability handling policy) conforme aux exigences de l'Annexe I du CRA, opposable en cas de contrôle.

Sources & références — Cliquez sur chaque source pour accéder directement à l'article original

- NIST NVD — CVE-2026-5194
- Industrial Cyber — CVE-2026-32746
- TheHackerWire — CVE-2026-41503
- SGS — ETSI Standards
- ETSI — Security Conference 2026
- CISA KEV — Catalog
- PurpleOps — CVE-2026-5194
- Hogan Lovells — CRA 2026
- VinciWorks — NIS2 & RED
- ReedSmith — RED & CRA