VEILLE & PRODUCTION INTELLECTUELLE

CyberWatch — Veille hebdomadaire

Production hebdomadaire de veille cybersécurité couvrant deux axes : vulnérabilités et incidents ciblant les systèmes embarqués, l'IoT et les réseaux d'opérateurs, et évolutions réglementaires cyber en cours à l'échelle internationale — notamment CRA, RED et ETSI. Chaque édition analyse les implications concrètes pour l'Afrique subsaharienne : exposition des infrastructures déployées, dynamiques réglementaires continentales et enjeux de souveraineté numérique.

4	3	2
SIGNAUX CRITIQUES	JALONS RÉGLEMENTAIRES	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

CVE CRITIQUE

CVE-2024-7399 — Samsung MagicINFO 9 Server | CVSS 8.8 — Ajouté KEV le 24/04/2026

Une faille de type ***path traversal***, sans authentification requise, permet à un attaquant distant d'uploader un fichier JSP arbitraire via l'endpoint ***/MagicInfo/servlet/SWUpdateFileUploader*** et de l'exécuter avec les privilèges SYSTEM du serveur. Samsung a publié un correctif en août 2024 — mais Huntress Labs a confirmé que la version 21.1050 demeure exploitable : le patch est incomplet ou cible une faille distincte. L'exploitation active est confirmée par CISA KEV (24/04/2026), avec des campagnes Mirai ciblant les instances exposées à des fins de DDoS et de persistance malveillante.

Correctif partiel — MagicINFO 9 Server v21.1050 : déconnecter du réseau public en urgence. Samsung MagicINFO équipe les affichages numériques de transport, retail, hôpitaux et lobbies d'entreprise. Sa présence est massive en Afrique subsaharienne via les déploiements d'affichage public Samsung.

CVE CRITIQUE

CVE-2025-29635 — D-Link DIR-823X | CVSS 7.5 — Ajouté KEV le 24/04/2026

Une injection de commandes OS via requête POST authentifiée vers **/goform/set_prohibiting** affecte les routeurs D-Link DIR-823X, en fin de support depuis novembre 2024. La faille est activement exploitée par le variant Mirai tuxnokill, détecté par Akamai depuis mars 2026, dans une campagne multi-cibles combinant CVE-2023-1389 (TP-Link Archer AX21) et un exploit RCE ciblant les routeurs ZTE ZXV10 H108L. Aucun correctif ne sera publié — le fabricant a définitivement arrêté le support.

Action immédiate : remplacer le dispositif — aucun patch n'est à attendre. Ces routeurs en fin de vie sont déployés à grande échelle dans les PME et réseaux résidentiels africains, où le cycle de renouvellement matériel est particulièrement lent.

■ FOCUS AFRIQUE — VEILLE EMBARQUÉE

Les deux CVE ajoutés au KEV le 24 avril 2026 cristallisent un risque structurel pour la région : les routeurs D-Link DIR-823X en fin de vie et les serveurs Samsung MagicINFO insuffisamment patchés représentent une part significative de l'infrastructure IoT déployée en Afrique subsaharienne. L'absence de mise à jour post-déploiement, combinée à une exposition directe sur l'internet sans segmentation de sécurité, transforme ces équipements en points d'entrée persistants pour les botnets Mirai. Dans les environnements à ressources opérationnelles limitées, le remplacement matériel immédiat reste rarement envisageable — la segmentation réseau et le blocage du trafic entrant sur les interfaces d'administration demeurent les seules mesures réalistes à court terme.

VEILLE EMBARQUÉE & IOT

Signaux 3 & 4 — Focus Afrique

CVE ACTIF

CVE-2026-32202 — Microsoft Windows Shell | CVSS 4.3 — Ajouté KEV le 28/04/2026

Une défaillance du mécanisme de protection dans le composant Windows Shell permet à un attaquant de forcer une authentification SMB et d'intercepter des hachages Net-NTLMv2 sans interaction de la victime — exploitation active confirmée. La faille résulte d'un correctif incomplet de CVE-2026-21510. Le groupe APT28 (Fancy Bear / Russie) l'exploite en la chaînant avec des failles MSHTML dans le cadre de campagnes d'espionnage ciblées. Échéance FCEB : 12 mai 2026.

Patch Microsoft disponible via Windows Update. Le score CVSS de 4.3 est trompeur : l'exploitation active par un APT étatique et le chaînage avec des failles MSHTML élèvent substantiellement le risque opérationnel réel.

BOTNET MIRAI

Campagne Mirai tuxnokill — IoT multi-cibles | Révélé par Akamai le 21/04/2026

Le variant Mirai tuxnokill exploite simultanément trois vecteurs sur des équipements IoT en fin de vie : CVE-2025-29635 (D-Link DIR-823X), CVE-2023-1389 (TP-Link Archer AX21) et un exploit RCE ciblant les routeurs ZTE ZXV10 H108L. Une fois le dispositif compromis, un script shell télécharge le binaire du bot, établit la persistance et l'enrôle dans un réseau de DDoS distribué. Première détection sur les honeypots Akamai en mars 2026 — activité en progression continue.

Akamai observe que les campagnes Mirai continuent de s'appuyer sur le code source originel, adapté par des acteurs de niveaux très variés. L'exploitation simultanée de trois vecteurs distincts marque néanmoins une progression dans la sophistication opérationnelle de cette vague.

■ FOCUS AFRIQUE — BOTNETS & INFRASTRUCTURE

La campagne tuxnokill trouve un terrain particulièrement favorable en Afrique subsaharienne : les routeurs TP-Link Archer AX21 et ZTE ZXV10 H108L représentent une part importante du parc CPE déployé par les opérateurs télécoms régionaux. Importés sans audit de sécurité préalable et rarement mis à jour après déploiement, ces équipements offrent une surface d'attaque persistante et largement accessible sur les plages IP africaines. La faille structurelle centrale reste l'absence de cadres d'homologation intégrant des exigences de sécurité sur les équipements terminaux et CPE : tant qu'aucune obligation de mise à jour ou de remplacement ne s'applique au parc déjà déployé, cette surface d'attaque continuera de croître mécaniquement avec le taux de pénétration des réseaux.

VEILLE RÉGLEMENTAIRE

Jalons CRA & Afrique

CRA JALON 01

CRA — 11 juin 2026 : J-38 — Notified Bodies & autorités notifiantes

Dans 38 jours, le Chapitre IV du Cyber Resilience Act (règlement UE 2024/2847) entre en application : chaque État membre devra avoir désigné ses autorités notifiantes et publié les procédures d'évaluation, de désignation et de notification des organismes d'évaluation de conformité (Notified Bodies). À partir de cette date, seuls les organismes dûment notifiés pourront conduire les évaluations de conformité CRA requises pour les produits à évaluation tierce obligatoire (Annexe VIII — catégories importantes et critiques). Toute procédure engagée auprès d'un organisme non encore notifié sera juridiquement sans effet.

La Commission européenne a publié le 3 mars 2026 un projet de lignes directrices CRA en consultation publique, visant à clarifier les obligations des fabricants, notamment pour les PME. Ces guidelines ne sont pas juridiquement contraignantes mais constituent la référence officielle d'interprétation.

ENISA JALON 02

ENISA CRA Single Reporting Platform — Phase de test avant septembre 2026

L'ENISA a contractualisé avec un prestataire le développement de la CRA Single Reporting Platform (SRP) — la plateforme centralisée par laquelle les fabricants devront notifier les vulnérabilités activement exploitées et les incidents sévères à partir du 11 septembre 2026. Une phase de test est prévue avant la mise en service. La plateforme adresse les notifications simultanément au CSIRT de l'État membre d'établissement principal du fabricant et à l'ENISA. Un acte délégué sur les conditions de rétention des notifications par les CSIRTs a été adopté (publication en attente de la période d'objection).

Échéances en cascade : 11/06/2026 — Notified Bodies opérationnels. 11/09/2026 — Reporting obligatoire via SRP (24h alerte, 72h rapport technique, 14j rapport final). 11/12/2027 — Application intégrale du CRA.

AFRIQUE JALON 03

Congo-Brazzaville — RGSSI validé le 21 avril 2026 | Première conférence cyber d'Afrique centrale annoncée

Le 21 avril 2026, l'ANSSI du Congo a réuni experts, techniciens et représentants des secteurs public et privé pour valider le Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) — futur cadre normatif national fixant les exigences de sécurité applicables aux infrastructures numériques publiques et privées. Le document, conforme aux standards internationaux, a été validé sous réserve d'intégration des amendements formulés, en prélude à son adoption officielle par l'ANSSI. Le 30 avril 2026, l'ANSSI a signé un accord avec OSIANE pour organiser la première conférence régionale des agences de cybersécurité d'Afrique centrale, prévue du 2 au 5 juin 2026 à Brazzaville.

Le RGSSI ambitionne d'instaurer un socle commun de règles, d'accompagner les structures dans la mise en conformité de leurs systèmes d'information et de renforcer la souveraineté numérique nationale.

■ ENJEUX AFRICAINS — CRA & CONFORMITÉ

Le Congo-Brazzaville n'est pas un cas isolé : la validation du RGSSI s'inscrit dans une dynamique continentale de structuration des cadres nationaux de cybersécurité, accélérée en partie par l'effet d'entraînement du CRA européen. Si le CRA ne s'applique pas aux marchés africains, les fabricants asiatiques et américains dont les équipements dominent ces marchés devront s'y conformer pour accéder à l'Europe — ce qui élèvera mécaniquement le niveau de sécurité de leurs produits pour tous les marchés. Les référentiels nationaux émergents en Afrique — dont le RGSSI congolais, inspiré des normes ISO 27001/27002 — trouvent dans le CRA et les normes ETSI un corpus technique internationalement reconnu sur lequel s'aligner, sans obligation légale directe mais avec un effet de convergence réel sur les pratiques et les exigences d'homologation.

SYNTHÈSE OPÉRATIONNELLE

Recommandations — Immédiat & Court terme

IMMÉDIAT
< 72h

Samsung MagicINFO 9 — CVE-2024-7399 (KEV 24/04/2026)

Le correctif Samsung étant incomplet selon Huntress Labs, déconnecter en priorité tout serveur MagicINFO 9 exposé sur l'internet public. Constituer un inventaire exhaustif des instances déployées — affichages publics, retail, transport, santé — et isoler celles qui ne peuvent être déconnectées immédiatement. Mettre en place un pare-feu applicatif bloquant les requêtes POST non authentifiées vers l'endpoint ***/MagicInfo/servlet/SWUpdateFileUploader***. Surveiller les logs IIS/Tomcat pour toute trace de fichier JSP uploadé hors processus nominal. Engager Samsung Security directement pour obtenir le statut du correctif complet et un calendrier de livraison.

IMMÉDIAT
< 48h

D-Link DIR-823X — CVE-2025-29635 (KEV 24/04/2026 — Fin de vie)

Ce dispositif est en fin de support — aucun correctif ne sera jamais publié. Le remplacement est la seule issue viable ; dans l'attente, désactiver l'accès à l'interface d'administration depuis le WAN, bloquer les ports 80/443 admin en entrée et segmenter sur VLAN isolé. Constituer un inventaire exhaustif des DIR-823X déployés en environnement PME et résidentiel professionnel, en priorisant les équipements dont l'interface de management est accessible depuis l'internet.

COURT
< 2 sem.

Windows Shell — CVE-2026-32202 (KEV 28/04/2026 — APT28)

Appliquer le patch Microsoft via Windows Update sur l'ensemble du parc, en priorisant les postes et serveurs ayant accès à des ressources sensibles — l'attribution à APT28 et le chaînage avec des failles MSHTML signalent une campagne d'espionnage ciblée. Renforcer la surveillance SIEM sur les comportements anormaux du processus explorer.exe et des shells Windows. Échéance FCEB fixée au 12 mai 2026 — les organisations non fédérales sont invitées à s'aligner sur ce calendrier.

COURT
< 1 mois

Botnet Mirai tuxnokill — Équipements IoT multi-vecteurs

Auditer l'ensemble du parc routeurs CPE pour identifier les TP-Link Archer AX21, ZTE ZXV10 H108L et D-Link DIR-823X exposés sur l'internet, et déployer les correctifs CVE-2023-1389 sur Archer AX21 si disponibles. Bloquer les connexions sortantes vers les ports caractéristiques des C&C Mirai — IRC et ports non standard — et intégrer les IoCs publiés par Akamai dans les règles IDS/IPS. Compléter par un audit de trafic réseau ciblant les flux DDoS caractéristiques des bots Mirai.

SYNTHÈSE OPÉRATIONNELLE

Recommandations stratégiques & Sources

STRAT.
Juin 2026

CRA — 11 juin 2026 : Notified Bodies opérationnels (J-38)

S'assurer dès maintenant que les organismes d'évaluation de conformité sollicités ont bien engagé leur procédure de notification auprès des autorités nationales compétentes — la désignation doit être formellement publiée avant le 11 juin 2026. Cartographier les produits relevant de l'évaluation tierce obligatoire (Annexe VIII CRA : catégories importantes et critiques) et initier sans délai les dossiers correspondants : SBOM complet, déclaration UE de conformité, rapport d'évaluation de sécurité. Pour les fabricants africains visant le marché européen, anticiper ces exigences dès la phase de design et établir un canal formel avec un Notified Body européen avant l'échéance.

STRAT.
Sept. 2026

CRA — 11 septembre 2026 : Reporting obligatoire via ENISA SRP

Mettre en place et tester la chaîne complète de notification avant le 11/09/2026 — alerte initiale sous 24h, rapport technique sous 72h, rapport final sous 14 jours — en identifiant formellement le CSIRT national compétent et en établissant un canal opérationnel avec lui. Connecter les équipes sécurité à la CRA Single Reporting Platform dès l'ouverture de la phase de test ENISA. Formaliser l'ensemble de ces procédures dans une politique de gestion des vulnérabilités conforme à l'Annexe I du CRA, opposable en cas de contrôle. Rappel : la non-conformité après le 11/09/2026 expose à des sanctions pouvant atteindre 10 millions EUR ou 2% du chiffre d'affaires annuel mondial.

Sources & références — Cliquez pour accéder aux articles originaux

- CISA KEV — CVE-2024-7399 & CVE-2025-29635
- The Hacker News — KEV 4 CVEs (24/04/2026)
- Akamai — Mirai tuxnokill (21/04/2026)
- The Hacker News — Mirai tuxnokill IoT
- SecurityOnline — CVE-2026-32202 APT28
- EUR-Lex — CRA Reporting Platform
- Hogan Lovells — CRA milestones 2026
- Abhishek Gautam — KEV Samsung + D-Link
- SecurityWeek — MagicINFO patch incomplet

Sources : NIST NVD | CISA KEV | The Hacker News | Akamai | EUR-Lex | ENISA | Hogan Lovells | Industrial Cyber | SecurityWeek