Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

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.

> *Cette veille est produite à titre personnel dans le cadre de mes travaux indépendants de recherche et d'analyse. Son contenu n'engage que son auteur et ne reflète la position d'aucune institution ou organisation.*

5	4	3
SIGNAUX CRITIQUES	JALONS RÉGLEMENTAIRES	FOCUS AFRIQUE

SOMMAIRE

Contenu de cette édition

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

INTRODUCTION

Pourquoi lire cette édition ?

La semaine du 4 au 10 mai 2026 concentre plusieurs signaux majeurs pour les équipes cybersécurité, les industriels, les fabricants d'équipements connectés, les opérateurs d'infrastructures critiques et les régulateurs.

Trois tendances dominent cette édition.

La première concerne les équipements de sécurité eux-mêmes. Une vulnérabilité critique dans PAN-OS de Palo Alto Networks expose certains pare-feux **PA-Series** et **VM-Series** à une exécution de code arbitraire à distance avec privilèges root, lorsque le portail User-ID Authentication Portal est exposé à des réseaux non fiables. Le fournisseur confirme une exploitation active et recommande des mesures de mitigation immédiates en attendant les correctifs.

La deuxième concerne le socle Linux. La vulnérabilité CVE-2026-31431, surnommée **Copy Fail**, affecte le noyau Linux via l'interface cryptographique **algif_aead**. Il s'agit d'une élévation locale de privilèges : un utilisateur local non privilégié peut obtenir les droits root sur un système vulnérable. Le risque est élevé dans les environnements serveurs, cloud, conteneurisés, mais aussi dans les produits embarqués et passerelles IoT reposant sur des noyaux Linux anciens ou non maintenus.

La troisième tendance illustre la convergence entre cybersécurité, IoT et conflit géopolitique. Check Point Research documente une intensification du ciblage de **caméras IP Hikvision** et **Dahua** dans plusieurs pays du Moyen-Orient et du Golfe, avec des infrastructures attribuées à des acteurs Iran-nexus. Ces caméras ne sont plus seulement des objets connectés vulnérables : elles deviennent des capteurs de renseignement, de reconnaissance et d'évaluation de dommages dans des contextes de conflit armé.

Ces signaux confirment une évolution profonde : la cybersécurité des équipements connectés ne peut plus être traitée comme un sujet purement technique. Elle concerne désormais les politiques d'achat, la certification, l'homologation, la conformité réglementaire, la résilience des infrastructures critiques et la souveraineté numérique.

VEILLE EMBARQUÉE & IOT

Signaux critiques — 1 & 2

CVE CRITIQUE

CVE-2026-0300 — Palo Alto Networks PAN-OS | CVSS 9.3 — Ajoutée au catalogue KEV le 06/05/2026

Une vulnérabilité critique de type débordement de tampon affecte le service **User-ID Authentication Portal**, également appelé **Captive Portal**, dans PAN-OS. Elle permet à un attaquant distant non authentifié d'exécuter du code arbitraire avec les privilèges **root** sur des pare-feux **PA-Series** et **VM-Series**, au moyen de paquets spécialement forgés. Aucune authentification ni interaction utilisateur n'est requise, ce qui rend l'exploitation particulièrement dangereuse lorsque le portail est exposé à Internet ou à des réseaux non fiables. Palo Alto Networks confirme une exploitation active limitée dans la nature et classe l'urgence au niveau le plus élevé.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

Selon les données rapportées par Shadowserver, plus de **5 800 firewalls VM-Series** seraient directement accessibles sur Internet, avec une concentration importante en Asie et en Amérique du Nord. La CISA a ajouté cette vulnérabilité à son catalogue **KEV — Known Exploited Vulnerabilities**, ce qui signifie qu'elle est considérée comme activement exploitée. Elle a fixé au **9 mai 2026** la date limite de remédiation obligatoire pour les agences fédérales civiles américaines relevant du périmètre **FCEB — Federal Civilian Executive Branch**. Cette obligation ne s'applique juridiquement qu'aux agences civiles fédérales américaines, mais elle constitue un signal fort de criticité pour toutes les organisations exposées.

*Aucun correctif n'était disponible au 6 mai 2026. Palo Alto Networks a annoncé une publication progressive des correctifs, avec une première vague attendue à partir du **13 mai 2026** et une seconde à partir du **28 mai 2026**. En attendant, la mitigation immédiate consiste à désactiver le **User-ID Authentication Portal** s'il n'est pas strictement nécessaire, ou à restreindre son accès aux seules zones internes de confiance. La désactivation s'effectue depuis : **Device > User Identification > Authentication Portal Settings > Enable Authentication Portal**. Les versions affectées incluent **PAN-OS 10.2, 11.1, 11.2 et 12.1**. **Prisma Access, Cloud NGFW et Panorama ne sont pas affectés**.*

Le risque est particulièrement sensible parce qu'il touche un équipement de frontière. Un pare-feu compromis cesse d'être un dispositif de protection : il devient une position d'observation, de pivot et de prépositionnement. Dans un environnement industriel, télécom ou gouvernemental, l'attaquant peut obtenir une visibilité stratégique sur les flux, les zones de sécurité, les règles de filtrage et les segments internes, y compris les réseaux OT. Cette vulnérabilité rappelle qu'un équipement de sécurité exposé doit lui-même être traité comme un actif critique, soumis à une surveillance, une segmentation et une gestion de configuration rigoureuses.

CVE ÉLEVÉ

CVE-2026-31431 — Linux Kernel "Copy Fail" | CVSS 7.8 — Ajoutée au catalogue KEV le 01/05/2026

La vulnérabilité **CVE-2026-31431**, surnommée **Copy Fail**, est une faille d'élévation locale de privilèges affectant le noyau Linux, plus précisément l'interface cryptographique **AF_ALG** et le composant **algif_aead**. Elle permet à un utilisateur local non privilégié de provoquer une écriture contrôlée de 4 octets dans le cache de pages du noyau, puis d'exploiter cette corruption pour obtenir des privilèges **root** sur un système vulnérable. Le caractère déterministe de l'exploitation — sans condition de course complexe ni adaptation spécifique à chaque distribution — rend cette faille particulièrement préoccupante dans les environnements Linux multi-utilisateurs, cloud, conteneurisés et embarqués. Microsoft la qualifie explicitement de vulnérabilité d'élévation locale de privilèges affectant plusieurs grandes distributions Linux, dont Red Hat, SUSE, Ubuntu et AWS Linux.

La vulnérabilité a été ajoutée le **1er mai 2026** au catalogue **KEV — Known Exploited Vulnerabilities** de la CISA, ce qui signifie qu'elle est considérée comme activement exploitée. La CISA a fixé au **15 mai 2026** la date limite de remédiation obligatoire pour les agences fédérales civiles américaines relevant du périmètre **FCEB — Federal Civilian Executive Branch**. Cette échéance ne s'applique juridiquement qu'à ces agences américaines, mais elle constitue un signal fort de criticité pour toutes les organisations utilisant Linux dans leurs infrastructures.

L'exploit public est particulièrement marquant par sa simplicité : il est souvent décrit comme un script Python de **732 octets** permettant d'obtenir les privilèges root sur des systèmes vulnérables. Des tests et analyses publics indiquent que l'exploitation fonctionne sur plusieurs distributions majeures, notamment **Ubuntu 24.04 LTS, Amazon Linux 2023, RHEL 10.1 et SUSE 16**, lorsque les versions concernées du noyau sont présentes. Il ne s'agit toutefois pas d'une vulnérabilité exploitable directement à distance :

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

l'attaquant doit déjà disposer d'un accès local non privilégié ou d'une capacité préalable d'exécution de code sur le système.

Des correctifs sont disponibles via les distributions concernées et les mises à jour du noyau Linux. Les systèmes exposés doivent être corrigés en priorité, avec redémarrage lorsque nécessaire afin de charger le noyau corrigé. Une vigilance particulière est requise pour les distributions de la famille RHEL, où certaines mitigations par blocage de module peuvent donner une fausse impression de protection lorsque le composant concerné est compilé directement dans le noyau. Dans ce cas, la priorité reste l'application du correctif noyau fourni par l'éditeur ou la distribution.

L'impact dépasse les serveurs classiques et les environnements cloud. Tout système Linux embarqué reposant sur un noyau vulnérable peut être concerné : passerelle IoT, équipement télécom, routeur CPE opérateur, appliance réseau, système industriel, plateforme Edge ou équipement embarqué spécialisé. Copy Fail rappelle une réalité souvent négligée : un produit embarqué n'est pas seulement vulnérable à cause de son application métier ou de son interface web. Il peut aussi l'être à cause de ses composants de base : noyau, bibliothèques, modules cryptographiques, services système et dépendances tierces. La capacité à identifier, suivre et corriger ces composants constitue précisément l'un des fondements des obligations de gestion des vulnérabilités et d'inventaire logiciel que le **Cyber Resilience Act** vient renforcer.

■ FOCUS AFRIQUE — PARE-FEUX, LINUX EMBARQUÉ ETREMÉDIATION

Les vulnérabilités **CVE-2026-0300** et **CVE-2026-31431** mettent en évidence un risque particulièrement sensible pour les organisations africaines qui exploitent des infrastructures réseau critiques, des équipements de sécurité périmétrique et des systèmes Linux embarqués.

Dans le cas de **CVE-2026-0300**, le risque porte sur les pare-feux **Palo Alto Networks PA-Series et VM-Series** lorsque le service **User-ID Authentication Portal** est activé et exposé à Internet ou à des réseaux non fiables. La criticité est élevée parce que la vulnérabilité permet une exécution de code à distance avec privilèges root, sans authentification ni interaction utilisateur. Palo Alto Networks précise toutefois que le risque est fortement réduit lorsque l'accès au portail est limité aux seules adresses internes de confiance ; Prisma Access, Cloud NGFW et Panorama ne sont pas affectés.

Pour les grandes entreprises, administrations, opérateurs télécoms, institutions financières et infrastructures critiques africaines, l'enjeu n'est pas seulement technique. Un pare-feu exposé et compromis peut devenir une position d'observation, de pivot et de prépositionnement vers les segments internes, y compris les environnements OT. Dans les contextes où les équipes sécurité sont réduites, où les fenêtres de maintenance sont rares et où les processus de patching sont parfois plus lents, l'absence initiale de correctif ou la difficulté d'appliquer rapidement les mitigations peut prolonger la fenêtre d'exposition.

Pour **Copy Fail — CVE-2026-31431**, l'enjeu est encore plus large. Il s'agit d'une élévation locale de privilèges affectant le noyau Linux, via le composant **algif_aead** de l'interface cryptographique **AF_ALG**. L'exploitation nécessite un accès local non privilégié ou une capacité préalable d'exécution de code, mais elle peut ensuite permettre d'obtenir les privilèges root sur un système vulnérable. Ubuntu qualifie cette faille de vulnérabilité locale d'élévation de privilèges, avec un score CVSS 7.8, et Microsoft confirme son impact sur plusieurs grandes distributions Linux utilisées dans les environnements cloud et serveurs.

Dans le contexte africain, cette vulnérabilité doit être lue à travers le prisme des équipements embarqués : passerelles IoT, routeurs CPE opérateurs, appliances réseau, équipements télécoms, systèmes industriels,

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

plateformes edge et dispositifs de supervision. Beaucoup de ces équipements reposent sur des noyaux Linux parfois anciens, peu documentés ou rarement mis à jour après leur déploiement. Le risque n'est donc pas uniquement l'exploitation immédiate de la faille, mais la difficulté à savoir rapidement quels équipements sont concernés, quelles versions du noyau sont utilisées, quels composants sont compilés dans le firmware, et si le fabricant fournit encore des correctifs.

Ces deux vulnérabilités rappellent une réalité structurante pour l'Afrique : la cybersécurité des infrastructures critiques dépend autant de la qualité des équipements que de la capacité à les inventorier, les configurer, les segmenter, les maintenir et les corriger dans la durée. Pour les organisations africaines, la priorité est donc double : réduire immédiatement l'exposition des services critiques accessibles depuis Internet, puis renforcer progressivement la gouvernance du cycle de vie des équipements connectés, notamment par l'inventaire des actifs, le suivi des versions firmware, la contractualisation du support sécurité et l'exigence de mises à jour correctives auprès des fournisseurs.

VEILLE EMBARQUÉE & IOT

Signaux 3, 4 & 5 — IoT, OT et convergence géopolitique

IOT SIGNAL 03

Caméras IP Hikvision & Dahua — Ciblage actif par des acteurs Iran-nexus | Check Point Research, mars 2026

Depuis le **28 février 2026**, Check Point Research documente une intensification du ciblage de caméras IP Hikvision et Dahua exposées sur Internet, à partir d'infrastructures attribuées à des acteurs **Iran-nexus**. Les activités observées concernent plusieurs pays du Moyen-Orient et du Golfe, notamment **Israël, Qatar, Bahreïn, Koweït, Émirats arabes unis, Liban et Chypre**. Cette campagne s'appuie sur l'exploitation ou la tentative d'exploitation de vulnérabilités connues affectant des équipements de vidéosurveillance et systèmes associés, notamment **CVE-2021-36260** sur Hikvision, **CVE-2017-7921** sur certains firmwares Hikvision, **CVE-2023-6895** sur des systèmes d'interphonie Hikvision, **CVE-2025-34067** sur Hikvision iSecure Center via désérialisation Fastjson, ainsi que **CVE-2021-33044** sur des produits Dahua. Le point critique n'est pas seulement l'existence de ces failles, mais leur persistance opérationnelle : plusieurs d'entre elles disposent de correctifs depuis plusieurs années, mais restent encore exploitables lorsque les équipements ne sont pas mis à jour.

Ces caméras ne sont pas uniquement ciblées pour de l'espionnage opportuniste. Dans un contexte de conflit hybride, elles peuvent devenir des capteurs de terrain utilisés pour la reconnaissance, l'observation de sites sensibles, l'évaluation des dommages après frappe et l'appui aux opérations suivantes. Nozomi Networks souligne que les caméras IP exposées, mal configurées ou non corrigées sont désormais utilisées dans la guerre moderne pour la surveillance avant frappe, le ciblage en temps réel et l'évaluation post-frappe, notamment lorsque des vulnérabilités anciennes restent présentes sur le terrain.

Le problème central n'est donc pas seulement l'existence de vulnérabilités, mais leur durée de vie réelle dans les équipements déployés. Des failles datant de 2017 et 2021 peuvent rester exploitables en 2026 lorsque les processus de mise à jour du firmware ne sont pas systématiques, lorsque les caméras sont directement exposées à Internet ou lorsque les politiques d'achat ne prévoient pas d'exigences de support sécurité. Ce cas illustre précisément pourquoi les référentiels comme ETSI EN 303 645 et le Cyber Resilience Act placent la gestion des mises à jour de sécurité, la correction des vulnérabilités et la maîtrise du cycle de vie produit au cœur des exigences applicables aux équipements connectés.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

OT/ICS SIGNAL 04

CISA CI Fortify — Doctrine nationale de résilience OT/ICS publiée le 06/05/2026

La CISA a lancé **CI Fortify**, une initiative nationale destinée à renforcer la résilience des infrastructures critiques face aux scénarios de crise cyber et de conflit géopolitique. Le message central est clair : les opérateurs d'infrastructures critiques doivent planifier leurs opérations en considérant que leurs dépendances tierces — télécommunications, Internet, fournisseurs, prestataires, services cloud et accès distants — peuvent devenir indisponibles, dégradées ou non fiables. La CISA recommande également de partir de l'hypothèse que des acteurs hostiles peuvent disposer d'un certain niveau d'accès aux réseaux OT dans un scénario de conflit.

CI Fortify structure deux objectifs prioritaires : **l'isolation** et **la récupération**. L'isolation consiste à maintenir les services essentiels même lorsque les systèmes OT doivent être séparés des réseaux IT, des connexions externes ou des dépendances fournisseurs. La récupération vise à restaurer rapidement les systèmes compromis ou dégradés, y compris en environnement isolé, avec des procédures documentées, testées et exécutables sans dépendance excessive aux outils externes. Plusieurs analyses de l'initiative soulignent que l'objectif n'est pas seulement de "résister à l'attaque", mais de continuer à fournir les services essentiels pendant une période prolongée, y compris en mode dégradé.

Les implications dépassent largement le territoire américain. Pour les opérateurs africains d'eau, d'énergie, de télécommunications, de transport et de services essentiels, CI Fortify fournit une grille de lecture très pertinente : les infrastructures critiques doivent pouvoir fonctionner même lorsque la connectivité est instable, les prestataires indisponibles, les accès distants coupés ou les systèmes partiellement compromis. Dans des environnements où les réseaux OT sont parfois peu segmentés, dépendants de fournisseurs étrangers ou insuffisamment supervisés, la résilience locale devient une priorité stratégique.

Concrètement, cela impose de renforcer la segmentation OT, de documenter les procédures manuelles de repli, de conserver localement les sauvegardes de configuration, de prévoir des communications hors bande, de tester les scénarios d'isolement et de s'assurer que les équipes peuvent maintenir le service essentiel sans dépendre entièrement d'Internet, du cloud ou d'un prestataire distant. CI Fortify rappelle ainsi une idée simple mais décisive : la cybersécurité OT ne se limite pas à empêcher l'intrusion ; elle consiste aussi à garantir la continuité du service lorsque l'environnement numérique devient dégradé, isolé ou partiellement hostile.

ICS SIGNAL 05

CISA ICS Advisories — 5 avis publiés le 05/05/2026 : Johnson Controls, ABB et Hitachi Energy

Le **5 mai 2026**, la CISA a publié cinq avis de cybersécurité industrielle concernant des produits de **Johnson Controls**, **ABB** et **Hitachi Energy**. Les avis couvrent notamment **Johnson Controls CEM AC2000**, **un produit Hitachi Energy**, ainsi que trois composants d'automatisation ABB : **ABB B&R PVI**, **ABB B&R Automation Runtime** et **ABB B&R Automation Studio**. Ces avis concernent des environnements utilisés dans des secteurs sensibles tels que l'énergie, les installations commerciales, les transports, la fabrication critique et les services gouvernementaux.

Pour **Johnson Controls CEM AC2000**, la faille signalée correspond à un problème de type **Uncontrolled Search Path Element**, souvent associé à un risque de **DLL hijacking**. Son exploitation pourrait permettre à un utilisateur standard d'élever ses privilèges sur la machine hôte. Côté ABB et Hitachi Energy, les avis rappellent que les composants d'ingénierie, d'automatisation et de configuration industrielle restent des cibles sensibles, car ils peuvent servir de point d'entrée vers les environnements OT lorsqu'ils sont mal segmentés, insuffisamment durcis ou utilisés depuis des postes d'ingénierie exposés.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

Ces publications s'inscrivent dans un contexte de surveillance renforcée des environnements **ICS/OT**. En mai 2026, l'ABW, service polonais de sécurité intérieure, a rendu publics des incidents survenus en 2025 dans plusieurs stations de traitement d'eau, où des attaquants ont obtenu, dans certains cas, un accès aux systèmes de contrôle industriel et la capacité de modifier des paramètres techniques d'équipements. Les vecteurs évoqués restent classiques mais critiques : mots de passe faibles, systèmes exposés directement à Internet et insuffisance de cloisonnement OT.

Pour les organisations africaines, le message est clair : les systèmes industriels ne doivent plus être considérés comme des environnements isolés par défaut. Même sans exposition directe volontaire à Internet, ils peuvent être atteints par des accès distants mal maîtrisés, des prestataires, des postes d'ingénierie compromis, des supports amovibles, des erreurs de segmentation ou des équipements de supervision insuffisamment durcis. La priorité est donc d'inventorier les actifs OT, de contrôler les accès distants, de segmenter les réseaux industriels, de durcir les postes d'ingénierie, de suivre les avis CISA ICS et d'intégrer ces vulnérabilités dans un processus régulier de gestion des risques industriels.

■ FOCUS AFRIQUE — CAMÉRAS IOT, OT & RÉSILIENCE

La campagne documentée autour des caméras **Hikvision** et **Dahua** a une résonance directe pour l'Afrique subsaharienne. Ces marques figurent parmi les plus visibles et les plus largement déployées dans les dispositifs de vidéosurveillance utilisés par les administrations, les espaces publics, les sites industriels, les ports, les aéroports, les banques et certaines infrastructures critiques. Les vulnérabilités documentées par Check Point Research ne dépendent pas de la localisation géographique de l'équipement : une caméra exposée, mal configurée ou non mise à jour reste exploitable, qu'elle soit installée au Moyen-Orient, en Europe ou en Afrique. Check Point a observé, depuis le 28 février 2026, une intensification du ciblage de caméras Hikvision et Dahua dans plusieurs pays, tandis que Nozomi Networks souligne que ces équipements peuvent désormais être utilisés dans des scénarios de reconnaissance avant frappe et d'évaluation post-frappe lorsque des failles anciennes restent non corrigées.

La leçon pour les organisations africaines est claire : une caméra IP ne doit plus être considérée comme un équipement périphérique sans enjeu stratégique. Lorsqu'elle est exposée à Internet, connectée au réseau interne ou installée à proximité d'un site sensible, elle peut devenir un capteur exploitable par un acteur hostile. Les politiques d'achat, de maintenance et d'exploitation doivent donc intégrer des exigences minimales : inventaire des caméras déployées, désactivation des accès inutiles, segmentation réseau, mise à jour régulière du firmware, changement des identifiants par défaut, journalisation des accès et contrôle des flux sortants.

La même logique s'applique aux environnements **OT**. L'initiative **CI Fortify** de la CISA, centrée sur l'isolation et la récupération des infrastructures critiques, est particulièrement pertinente pour les opérateurs africains d'eau, d'énergie, de télécommunications, de transport et de services essentiels. Elle rappelle que les opérateurs doivent planifier leurs opérations en considérant que les dépendances tierces — Internet, télécommunications, prestataires, accès distants, cloud ou fournisseurs — peuvent devenir indisponibles, dégradées ou non fiables en situation de crise. Pour des infrastructures où les ressources de supervision sont parfois limitées et où les dépendances techniques externes peuvent être fortes, la résilience locale devient un enjeu stratégique.

Dans cette perspective, la première conférence régionale des agences de cybersécurité d'Afrique centrale, prévue du **2 au 5 juin 2026 à Brazzaville**, en marge de la 10e édition d'OSIANE, constitue une occasion importante d'inscrire les enjeux **IoT, OT et résilience des infrastructures critiques** dans les agendas institutionnels régionaux. Plusieurs sources annoncent que cette rencontre doit réunir institutions spécialisées, experts et décideurs autour de la cybersécurité en Afrique centrale, dans un contexte de montée des cybermenaces et de recherche d'harmonisation des stratégies régionales.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

SYNTHÈSE

Cinq signaux, une dynamique commune

La semaine S19 ne présente pas cinq problèmes indépendants. Elle révèle une tendance de fond : la cybersécurité des équipements connectés repose désormais sur des chaînes de composants, de services et de dépendances que l'opérateur final ne maîtrise pas toujours. Qu'il s'agisse d'un pare-feu de périmètre, d'un noyau Linux embarqué, d'une caméra de surveillance, d'un composant industriel ou d'un routeur CPE, le risque ne se limite plus à l'équipement visible. Il concerne aussi le firmware, le noyau, les bibliothèques, les modules cryptographiques, les services d'administration, les mécanismes de mise à jour et les dépendances fournisseurs.

CVE-2026-0300 illustre que l'équipement de sécurité lui-même peut devenir le maillon faible. Une vulnérabilité critique dans le service User-ID Authentication Portal de PAN-OS peut permettre à un attaquant distant non authentifié d'exécuter du code avec privilèges root sur certains pare-feux PA-Series et VM-Series lorsque le service est exposé à des réseaux non fiables. Dans ce scénario, le pare-feu cesse d'être uniquement une barrière de protection : il devient potentiellement une position d'observation, de pivot et de prépositionnement vers les segments internes.

Copy Fail — CVE-2026-31431 rappelle que les composants de base, comme le noyau Linux, peuvent porter des vulnérabilités critiques pendant plusieurs années lorsqu'ils ne sont pas correctement suivis. La faille affecte l'interface cryptographique AF_ALG, via le composant algif_aead, et permet à un utilisateur local non privilégié d'obtenir des privilèges root sur un système vulnérable. Elle n'est pas exploitable directement à distance, mais elle devient très dangereuse dès qu'un attaquant dispose d'un premier accès local ou d'une capacité d'exécution de code.

La campagne visant des caméras **Hikvision** et **Dahua** montre, de son côté, que les vulnérabilités anciennes restent opérationnellement dangereuses lorsqu'elles persistent dans des équipements déployés. Le problème n'est pas uniquement l'existence de failles connues ; il réside dans leur maintien sur le terrain, parfois plusieurs années après la publication des correctifs. Dans un contexte de conflit hybride, une caméra IP exposée ou non corrigée peut devenir un capteur de reconnaissance, d'observation ou d'appui aux opérations, au lieu de rester un simple outil de vidéosurveillance.

Les avis **CISA ICS** du 5 mai 2026 confirment que les environnements industriels restent soumis à une pression continue. Les vecteurs sont souvent connus : authentification insuffisante, contrôle d'accès faible, mauvaises configurations, composants non mis à jour, postes d'ingénierie exposés, accès distants mal maîtrisés ou segmentation insuffisante. Cette réalité concerne directement les infrastructures critiques, où une vulnérabilité ne menace pas seulement des données, mais aussi la continuité du service, l'intégrité des processus et parfois la sécurité physique.

CI Fortify synthétise la réponse stratégique proposée par la CISA face à cette évolution. L'initiative invite les opérateurs d'infrastructures critiques à planifier leurs opérations en considérant que les dépendances tierces — télécommunications, Internet, fournisseurs, services cloud, accès distants — peuvent devenir indisponibles ou non fiables en situation de crise. Elle met au centre deux objectifs opérationnels : l'isolation et la récupération.

Pour les régulateurs, les fabricants et les laboratoires d'évaluation, la leçon est structurante : ces vulnérabilités montrent les limites d'une approche fondée uniquement sur la conformité initiale ou la déclaration fournisseur. La sécurité d'un équipement connecté doit être pensée sur tout son cycle de vie : conception sécurisée, inventaire logiciel, suivi des composants tiers, publication des correctifs, mécanismes de mise à jour, durée de support, documentation technique et capacité de remédiation. C'est précisément cette logique que les cadres **CRA, RED Cyber et ETSI** cherchent à renforcer à l'échelle européenne, et que les autorités africaines d'homologation peuvent commencer à structurer dès maintenant dans leurs propres référentiels.

La dynamique commune de cette semaine est donc claire : le risque cyber ne réside plus seulement dans l'attaque visible, mais dans la combinaison entre équipements connectés, dépendances tierces, vulnérabilités persistantes et cycles de vie mal maîtrisés. Pour l'Afrique, l'enjeu est stratégique : bâtir des infrastructures numériques et industrielles capables non seulement de se connecter, mais aussi de se maintenir, se corriger, s'isoler et continuer à fonctionner lorsque l'environnement numérique devient incertain.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

VEILLE RÉGLEMENTAIRE

Jalons CRA, RED & ETSI — J-32 et au-delà

CRA JALON 01

CRA — 11 juin 2026 : notification des organismes d'évaluation de conformité

À partir du **11 juin 2026**, le **Chapitre IV du Cyber Resilience Act** entre en application. Ce jalon concerne la notification des organismes d'évaluation de conformité, c'est-à-dire les futurs **Notified Bodies** appelés à intervenir pour certains produits numériques soumis à une évaluation tierce. Il ne marque pas encore l'application générale du CRA, prévue le **11 décembre 2027**, mais il prépare l'écosystème institutionnel et technique nécessaire à sa mise en œuvre. Les obligations de notification des vulnérabilités activement exploitées et des incidents graves, prévues à l'**article 14**, commenceront quant à elles le **11 septembre 2026**.

Pour les fabricants concernés, l'enjeu est d'anticiper dès maintenant la conformité : identifier les produits susceptibles d'entrer dans les catégories importantes ou critiques, préparer la documentation technique, structurer la gestion des vulnérabilités et vérifier que les organismes sollicités seront bien notifiés pour le périmètre CRA applicable. Cette étape est essentielle pour sécuriser la validité des futures évaluations de conformité et éviter d'engager des démarches auprès d'acteurs non habilités.

CRA JALON 02

CRA — Article 14 : notification des vulnérabilités à partir du 11/09/2026

À partir du **11 septembre 2026**, l'**article 14 du Cyber Resilience Act** imposera aux fabricants de notifier les vulnérabilités activement exploitées et les incidents graves affectant la sécurité de leurs produits numériques. Cette obligation entrera en vigueur avant l'application générale du règlement, prévue le **11 décembre 2027**. Le calendrier est contraignant : première alerte sous **24 heures**, notification complète sous **72 heures**, puis rapport final au plus tard **14 jours après la disponibilité d'une mesure corrective** pour les vulnérabilités activement exploitées. Pour les incidents graves, le rapport final devra être transmis dans un délai d'un mois.

*Concrètement, les fabricants devront disposer d'un processus formalisé de veille, qualification, notification, traitement et communication des vulnérabilités. **Copy Fail** illustre parfaitement cet enjeu : lorsqu'un composant tiers critique comme le noyau Linux est affecté par une vulnérabilité activement exploitée, le fabricant doit pouvoir identifier rapidement les produits concernés, les versions affectées et les mesures de correction ou de mitigation à communiquer aux utilisateurs. Sans inventaire logiciel, sans SBOM, sans politique de support documentée et sans processus de gestion des vulnérabilités, cette réponse devient difficilement soutenable dans les délais imposés par le CRA.*

RED JALON 03

RED — Abrogation du règlement délégué 2022/30 au 11/12/27 : transition vers le CRA

La Commission européenne a confirmé l'abrogation du **règlement délégué (UE) 2022/30**, dit **RED Cyber**, avec effet au **11 décembre 2027**, date d'application complète du **Cyber Resilience Act**. L'objectif est d'éviter un chevauchement entre les exigences de cybersécurité de la directive RED et celles du CRA, qui deviendra le cadre horizontal de référence pour les produits comportant des éléments numériques, y compris les équipements radioélectriques.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

Jusqu'au **10 décembre 2027**, les équipements radio concernés restent soumis aux exigences cybersécurité RED activées par le règlement délégué 2022/30, notamment les exigences liées aux articles **3.3 d, e et f** : protection des réseaux, protection des données personnelles et de la vie privée, et protection contre la fraude. À partir du **11 décembre 2027**, ces exigences basculeront dans le cadre CRA. Les normes **EN 18031-1, EN 18031-2 et EN 18031-3** conserveront donc leur importance pendant la période de transition, avant d'être progressivement remplacées ou complétées par les normes harmonisées développées pour le CRA.

Pour les fabricants d'équipements radioélectriques, le message est clair : la conformité RED Cyber reste pleinement applicable jusqu'à la bascule de décembre 2027, mais la migration vers le CRA doit être anticipée dès maintenant. Les cycles de conception, d'essais, de certification et de mise sur le marché dans l'industrie radio peuvent être longs ; attendre 2027 pour intégrer les exigences CRA exposerait les fabricants à des retards de conformité, à des surcoûts et à des difficultés de maintien sur le marché européen.

ETSI JALON 04

ETSI — Standards verticaux CRA en consultation publique | 18 catégories de produits

L'**ETSI** conduit actuellement des consultations ouvertes sur des projets de standards verticaux liés au **Cyber Resilience Act**. Ces drafts couvrent **18 catégories de produits numériques**, notamment les routeurs, modems, commutateurs, systèmes d'exploitation, navigateurs, VPN, SIEM, gestionnaires de réseau, gestionnaires de démarrage, interfaces réseau, PKI et autres composants d'infrastructure. Les documents sont accessibles via l'**ETSI Open Area** et restent des versions intermédiaires susceptibles d'évoluer avant leur publication finale.

Ces standards traduiront les exigences générales du CRA en critères techniques par catégorie de produit. Une fois harmonisés et publiés au **Journal officiel de l'Union européenne**, ils pourront donner une **présomption de conformité** aux fabricants qui les appliquent. Leur publication est attendue au second semestre 2026, avec une échéance cible autour du **30 octobre 2026** pour plusieurs travaux de normalisation.

Pour les fabricants et laboratoires de test, ces drafts doivent déjà être suivis de près. Ils ne constituent pas encore des normes harmonisées définitives, mais ils donnent une orientation claire sur les futurs critères d'évaluation : conception sécurisée, configuration par défaut, gestion des vulnérabilités, mises à jour, documentation technique et maîtrise du cycle de vie. Pour les équipements IoT, radio, réseau et industriels, ils deviennent une base de préparation stratégique avant l'application complète du CRA.

■ ENJEUX AFRICAINS — CRA, RED & CONVERGENCE RÉGLEMENTAIRE

La convergence progressive entre le cadre **RED Cyber** et le **Cyber Resilience Act** crée une opportunité stratégique pour les régulateurs africains. À partir du **11 décembre 2027**, le règlement délégué **(UE) 2022/30** sera abrogé afin d'éviter les chevauchements avec le CRA, qui deviendra le cadre européen de référence pour la cybersécurité des produits comportant des éléments numériques, y compris les équipements radioélectriques. Cette évolution offre aux autorités africaines une base plus cohérente pour structurer leurs propres exigences d'homologation autour d'un corpus unique : sécurité par conception, gestion des vulnérabilités, mises à jour, documentation technique et maîtrise du cycle de vie.

Pour l'Afrique, l'enjeu n'est pas de copier mécaniquement le modèle européen, mais de s'en inspirer intelligemment. Les fabricants internationaux qui ciblent le marché européen devront progressivement intégrer les exigences CRA dans leurs produits. Cette dynamique peut bénéficier aux marchés africains, à condition que

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

les autorités locales traduisent ces exigences dans leurs procédures d'importation, d'homologation, de contrôle et d'achat public.

La campagne sur les caméras Hikvision et Dahua illustre l'effet inverse : lorsque des équipements massivement déployés ne sont pas soumis à des obligations vérifiables de mise à jour et de support sécurité, des vulnérabilités anciennes peuvent rester exploitables pendant des années. Pour les régulateurs africains, la leçon est claire : la conformité initiale ne suffit plus. La cybersécurité des équipements connectés doit être suivie sur tout le cycle de vie du produit.

IMPLICATIONS

Ce que ces signaux changent concrètement

Les vulnérabilités de la semaine ne concernent pas uniquement les grands marchés européens ou américains. Elles ont une résonance directe pour l'Afrique subsaharienne et pour toutes les organisations qui conçoivent, achètent, déploient ou régulent des équipements connectés.

Pour les décideurs, le premier message est simple : un pare-feu vulnérable n'est pas un sujet technique secondaire, c'est un risque stratégique. Si le composant chargé de protéger le réseau est compromis, toute la posture de sécurité est fragilisée. Les caméras IP, routeurs, CPE et objets connectés doivent également être considérés comme des actifs sensibles : ils peuvent devenir des points d'entrée, des capteurs d'espionnage ou des relais d'attaque. Enfin, le cadre européen avance rapidement : le **Chapitre IV du CRA** s'applique à partir du **11 juin 2026**, les obligations de notification de l'**article 14** entreront en vigueur le **11 septembre 2026**, et l'application générale du règlement est prévue le **11 décembre 2027**.

Pour les fabricants d'équipements connectés, la priorité est de structurer une véritable gouvernance de cybersécurité produit. Chaque fabricant doit pouvoir identifier les composants logiciels intégrés dans ses produits, suivre les vulnérabilités qui les affectent, produire des correctifs, les distribuer de manière sécurisée et documenter la durée de support. Le SBOM, la gestion des vulnérabilités, la sécurité des mises à jour et la traçabilité des versions ne sont plus de simples bonnes pratiques : ils deviennent les fondations de la conformité CRA. Les cas Hikvision et Dahua rappellent qu'un correctif disponible mais non appliqué ne réduit pas réellement le risque sur le terrain.

Pour les laboratoires de test et d'évaluation, ces signaux fournissent des cas pratiques directement exploitables. **Copy Fail** peut servir à vérifier la version du noyau Linux, les modules cryptographiques exposés et la maturité du processus de correction. Les campagnes visant des caméras IP montrent l'importance de tester le firmware, les interfaces d'administration, l'authentification, l'exposition réseau, les flux sortants et les mécanismes de mise à jour. Les futurs protocoles d'évaluation devront se rapprocher davantage des conditions réelles de déploiement : inventaire logiciel, vulnérabilités connues, durcissement des services, signature des mises à jour, journalisation et documentation de sécurité.

Pour les régulateurs et autorités d'homologation, cette semaine confirme qu'il ne suffit plus de vérifier la conformité radio, la compatibilité électromagnétique ou l'utilisation correcte du spectre. Les équipements connectés doivent aussi être évalués sous l'angle de la cybersécurité : exposition réseau, authentification, chiffrement, mises à jour, absence de fonctions cachées ou malveillantes, gestion du firmware, documentation de support et cycle de vie. Pour l'Afrique, l'enjeu n'est pas de copier mécaniquement l'Europe, mais d'adapter ces référentiels aux réalités locales : moyens des laboratoires, maturité des opérateurs, disponibilité des fabricants, contraintes d'importation, niveau de risque des équipements et criticité des infrastructures.

Pour les opérateurs et acheteurs d'équipements, le prix ne peut plus être le seul critère d'acquisition. La durée de support déclarée, la politique de mise à jour, la transparence sur les vulnérabilités, la disponibilité des correctifs, la documentation technique et la capacité à désactiver les services non nécessaires doivent devenir des critères contractuels. Un équipement bon marché dont le firmware n'est jamais maintenu peut coûter, à terme, bien plus cher que le différentiel de prix initial.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

SYNTHÈSE OPÉRATIONNELLE

Recommandations — Immédiat, court terme & stratégique

Mesures immédiates — 48 à 72 heures

IMMÉDIAT < 48h

PAN-OS — CVE-2026-0300 (KEV 06/05/2026 — Aucun patch disponible)

Vérifier si le **User-ID Authentication Portal** est activé et exposé à Internet ou à des réseaux non fiables. Si le service n'est pas indispensable, le désactiver. S'il est nécessaire, restreindre strictement son accès aux seules zones internes de confiance et réduire l'exposition des pages de réponse sur les interfaces concernées. Surveiller l'advisory Palo Alto Networks et appliquer les correctifs dès leur disponibilité. **Prisma Access, Cloud NGFW et Panorama ne sont pas affectés**.

IMMÉDIAT < 72h

Linux Kernel 'Copy Fail' — CVE-2026-31431 (KEV 01/05/2026 — Deadline FCEB 15/05/2026)

Inventorier les systèmes Linux afin d'identifier les noyaux vulnérables, puis appliquer les correctifs selon les recommandations des distributions. Prioriser les environnements cloud, Kubernetes, serveurs multi-utilisateurs et produits embarqués Linux. Pour les distributions de la famille **RHEL**, ne pas se limiter à une mitigation par blocage de module si le composant concerné est compilé dans le noyau : la priorité reste l'application du correctif noyau. Pour les équipements OEM non maintenus, évaluer une mise à niveau hors cycle ou un remplacement lorsque le correctif n'est pas disponible.

Mesures à court terme — Une à deux semaines

COURT < 1 sem.

Caméras IP Hikvision & Dahua — 5 CVE exploitées activement

Appliquer les correctifs disponibles pour les vulnérabilités connues affectant les produits Hikvision et Dahua ciblés. Aucune caméra IP ne doit être directement accessible depuis Internet : l'accès doit passer par un VPN, une passerelle sécurisée ou une architecture zero trust. Réaliser un inventaire des caméras déployées dans les bâtiments sensibles, sites industriels et infrastructures critiques. Segmenter les caméras sur un VLAN dédié, surveiller les flux sortants et retirer tout accès inutile vers les réseaux bureautiques ou OT.

COURT < 2 sem.

CI Fortify & Avis ICS CISA — Audit isolation OT et revue des dépendances

Initier une revue des dépendances tierces des systèmes OT : télécommunications, fournisseurs, services cloud, outils de maintenance à distance et accès prestataires. Documenter les actifs OT nécessaires à chaque service essentiel et établir un plan de continuité en mode isolé. Tester la capacité à fonctionner sans connectivité externe pendant au moins 72 heures. Consulter les avis ICS publiés par la CISA le **5 mai 2026** et vérifier l'exposition éventuelle des produits **Johnson Controls, ABB et Hitachi Energy** dans le parc déployé.

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

Mesures stratégiques — 2026 à 2027

STRAT. Juin 2026

CRA — 11 juin 2026 : Notified Bodies opérationnels (J-32)

Identifier les produits susceptibles de relever d'une évaluation tierce obligatoire au titre du CRA et préparer les dossiers de conformité : documentation technique, analyse de sécurité, inventaire logiciel, SBOM et processus de gestion des vulnérabilités. Les fabricants visant le marché européen doivent vérifier que les organismes sollicités seront bien notifiés pour le périmètre CRA applicable et intégrer ces exigences dès le cycle de développement produit.

STRAT. Sept. 2026

CRA — Article 14 : mettre en place la chaîne de notification des vulnérabilités

Mettre en place et tester la chaîne de notification avant le **11 septembre 2026** : détection, qualification, alerte initiale, notification complète, suivi des mesures correctives et rapport final. Identifier les canaux de notification compétents et formaliser ces procédures dans une politique de gestion des vulnérabilités. Pour les fabricants, l'enjeu est de pouvoir répondre rapidement à trois questions : quels produits sont concernés, quelles versions sont affectées et quelles mesures de correction ou de mitigation peuvent être communiquées.

STRAT. Continu

Politique d'achat & cycle de vie des équipements connectés

Intégrer dans les politiques d'achat des critères contractuels de cybersécurité : durée minimale de support sécurité, mécanisme de mise à jour sécurisée, publication des vulnérabilités affectant le produit, documentation technique, désactivation des services non nécessaires et engagement de correction. Réaliser un audit régulier du firmware des équipements IoT, de surveillance, d'automatisation et de supervision. Une vulnérabilité ancienne encore exploitable en 2026 n'est pas une fatalité technique : c'est souvent l'indicateur d'un cycle de vie insuffisamment maîtrisé.

SOURCES & RÉFÉRENCES

Sources — Cliquez pour accéder aux articles originaux

L'ensemble des informations contenues dans cette édition est issu de sources publiques primaires. Les liens ci-dessous permettent d'accéder directement aux articles et avis originaux pour approfondir chaque signal.

CVE-2026-0300 — PALO ALTO PAN-OS

- Palo Alto Networks — Advisory officiel
- The Hacker News — PAN-OS CVE-2026-0300
- BleepingComputer — PAN-OS zero-day exploité
- Rapid7 — ETR CVE-2026-0300
- Wiz — Blog CVE-2026-0300
- CISA KEV — Catalog (CVE-2026-0300 & CVE-2026-31431)

CVE-2026-31431 — LINUX KERNEL 'COPY FAIL'

- CERT-EU — Advisory CVE-2026-31431
- Microsoft Security Blog — Copy Fail deep dive
- Ubuntu Security — Copy Fail fixes
- Sysdig — Copy Fail : root en secondes

Abdoul Karim Mamani Malam Goga
Cybersecurity & RF Compliance | Radio · IoT · Embedded Security · Critical Infrastructure | RED · CRA · ETSI

CAMÉRAS IP HIKVISION & DAHUA — CAMPAGNE IRAN-NEXUS

Check Point Research — Caméras Iran-nexus
Cybersecurity Dive — Iran cible les caméras IP
Elisity — IoT camera security lessons

OT / ICS — CI FORTIFY & AVIS INDUSTRIELS

CISA — CI Fortify Initiative
SecurityWeek — CI Fortify (06/05/2026)
CISA ICS — Johnson Controls CEM AC2000 (ICSA-26-125-05)
CISA ICS — ABB B&R Automation Runtime (ICSA-26-125-03)
CISA ICS — ABB B&R PVI (ICSA-26-125-02)
CISA ICS — ABB B&R Automation Studio (ICSA-26-125-04)
CISA ICS — ABB PCM600 (ICSA-26-120-02)

RÉGLEMENTATION — CRA, RED & ETSI

Hogan Lovells — CRA 2026 milestones
Compliance & Risks — ETSI CRA standards
Global Norm — RED abrogation & normes EN 18031

AFRIQUE — VEILLE RÉGLEMENTAIRE & INSTITUTIONNELLE

Africa Cybersecurity Mag — ANSSI Congo / OSIANE juin 2026