Procédure de mise à jour firmware

Référence	Version	Date	Catégorie
PROC-CYB-002	v1.0	Avril 2025	Cybersécurité

Les vulnérabilités dans les firmwares des équipements de sécurité sont une cible privilégiée des cyberattaquants. Des failles critiques sont régulièrement découvertes dans les caméras IP, NVR et équipements réseau. Mileo Technology assure une veille active et applique les mises à jour selon une procédure structurée garantissant la continuité de service et la traçabilité des versions déployées.

---

01. Veille sur les vulnérabilités

Mileo Technology réalise une veille hebdomadaire sur les sources suivantes : bulletins de sécurité ANSSI / CERT-FR, National Vulnerability Database (NVD) du NIST, bulletins de sécurité des constructeurs partenaires (Axis, Hikvision, Dahua, Genetec, Milestone, etc.), listes de diffusion spécialisées en sécurité IoT et vidéosurveillance.

Les vulnérabilités sont identifiées par leur identifiant CVE (Common Vulnerabilities and Exposures) et évaluées selon leur score CVSS v3.1. Un tableau de suivi des vulnérabilités actives est maintenu par le référent cybersécurité et communiqué mensuellement aux chefs de projet.

Les alertes critiques (score CVSS ≥ 9.0) font l'objet d'une notification immédiate à l'ensemble des équipes techniques, avec identification des installations potentiellement concernées dans les 24 heures.

---

02. Priorisation selon la criticité

Les mises à jour sont priorisées selon le score CVSS de la vulnérabilité corrigée : critique (CVSS ≥ 9.0) — déploiement sous 24 heures ; haute (CVSS 7.0-8.9) — déploiement sous 72 heures ; moyenne (CVSS 4.0-

6.9) — déploiement dans le prochain cycle de maintenance préventive ou sous 30 jours ; basse (CVSS < 4.0) — intégrée au cycle normal de maintenance.

La criticité fonctionnelle du site concerné module également la priorité : un site classé sensible (établissement bancaire, infrastructure critique, bâtiment gouvernemental) bénéficie d'un délai réduit de moitié par rapport aux délais standard. Cette classification est documentée dans la fiche client.

---

03. Environnement de test

Avant tout déploiement sur un site client, les mises à jour majeures de firmware (changement de version principale) sont testées sur un équipement de référence identique au sein du laboratoire de Mileo Technology. Les tests vérifient le maintien des fonctionnalités critiques : détection de mouvement, enregistrement, accès à distance, intégration VMS.

Pour les mises à jour mineures (correctifs de sécurité sans changement fonctionnel majeur), le test peut être réalisé directement sur une caméra ou un NVR non critique du site, préalablement au déploiement généralisé. Les résultats des tests sont documentés.

---

04. Procédure de rollback

Avant toute mise à jour, la version du firmware en place est documentée et le fichier de configuration actuel est sauvegardé. Certains équipements permettent de conserver l'ancienne version du firmware pour un rollback rapide ; cette fonctionnalité est utilisée lorsqu'elle est disponible.

En cas de dysfonctionnement constaté après mise à jour, le technicien dispose d'une procédure de retour arrière documentée par type d'équipement. Le délai maximum de retour à la normale après un rollback est de 2 heures pour les équipements critiques. L'incident est documenté et remonté au référent cybersécurité.

---

05. Fenêtres de maintenance et traçabilité

Les mises à jour sont réalisées pendant les fenêtres de maintenance définies contractuellement avec le client (généralement en dehors des heures d'exploitation du site). Pour les mises à jour urgentes de vulnérabilités critiques, le client est informé de la nécessité d'une intervention en urgence.

> **Chaque mise à jour est tracée dans le registre de configuration du site : équipement concerné, ancienne version, nouvelle version, date d'intervention, technicien responsable. Ce registre est intégré au dossier de configuration client et consultable sur demande.**

Boulevard de Courcelles, 75008 Paris — hello@mileotech.com