Politique de gestion des vulnérabilités

Référence	Version	Date	Catégorie
POL-CYB-005	v1.0	Mars 2025	Cybersécurité

La gestion proactive des vulnérabilités est au cœur de la cybersécurité des systèmes de vidéosurveillance. Des centaines de vulnérabilités sont découvertes chaque année dans les équipements de sécurité physique, dont certaines permettent une prise de contrôle complète à distance. Mileo Technology s'engage à identifier, évaluer et corriger les vulnérabilités affectant les systèmes de ses clients dans des délais définis selon leur criticité.

---

01. Sources de veille

Mileo Technology s'appuie sur un ensemble diversifié de sources de veille en vulnérabilités : les alertes et avis de sécurité du CERT-FR (ANSSI), la National Vulnerability Database (NVD) du NIST avec ses identifiants CVE, les bulletins de sécurité des constructeurs partenaires publiés sur leurs portails officiels, les listes de diffusion spécialisées (Full Disclosure, OSS-Security) et les veilles sectorielles publiées par des organismes spécialisés en sécurité des systèmes physiques.

Un abonnement aux alertes de chaque constructeur dont les équipements sont déployés chez nos clients est maintenu. Le référent cybersécurité effectue une revue hebdomadaire de l'ensemble de ces sources et qualifie les nouvelles vulnérabilités dans un registre centralisé.

---

02. Classification des vulnérabilités

Les vulnérabilités sont classifiées en quatre niveaux selon leur score CVSS v3.1 : Critique (score ≥ 9.0) — exploitabilité immédiate, impact maximal, souvent associée à une preuve de concept publique ; Haute

(score 7.0-8.9) — exploitabilité probable, impact significatif ; Moyenne (score 4.0-6.9) — exploitation nécessitant des conditions particulières ; Basse (score < 4.0) — impact limité ou exploitation très difficile.

La classification CVSS est complétée par une analyse contextuelle : présence d'un exploit public, exposition du système à Internet, sensibilité du client concerné. Cette analyse peut conduire à reclasser une vulnérabilité à un niveau supérieur à celui suggéré par son seul score CVSS.

---

03. Délais de correction

Les délais de correction imposés selon la classification sont : Critique — 24 heures maximum à compter de la disponibilité d'un correctif ; Haute — 72 heures maximum ; Moyenne — 30 jours maximum ou lors du prochain cycle de maintenance ; Basse — 90 jours maximum ou lors de la prochaine maintenance annuelle.

Ces délais sont mesurés à partir de la disponibilité d'un correctif officiel du constructeur, et non à partir de la publication de la vulnérabilité. Le référent cybersécurité informe les clients concernés dans les 4 heures suivant l'identification d'une vulnérabilité Critique affectant leurs systèmes.

---

04. Vulnérabilités sans correctif disponible

Lorsqu'une vulnérabilité est identifiée sans correctif disponible (zero-day ou correctif en attente de publication), des mesures compensatoires sont immédiatement mises en place : isolation réseau renforcée de l'équipement concerné, restriction des accès, surveillance accrue des journaux, désactivation des fonctionnalités exposées si possible.

La situation est formellement documentée dans le registre des vulnérabilités, avec les mesures compensatoires appliquées, la date d'identification et le suivi du statut du correctif. Le client est informé de la situation et des mesures prises. Lorsque le risque résiduel est jugé inacceptable et qu'aucune mesure compensatoire n'est suffisante, le remplacement de l'équipement est recommandé.

---

05. Suivi et reporting

Un rapport mensuel de gestion des vulnérabilités est produit, récapitulant les vulnérabilités identifiées, leur statut de traitement et les délais respectés. Ce rapport est partagé avec la direction et, pour les clients disposant d'un contrat de cybersécurité, avec le responsable sécurité du client.

> **Les indicateurs clés suivis sont : délai moyen de correction par niveau de criticité, pourcentage de vulnérabilités traitées dans les délais, nombre de vulnérabilités en attente de correctif. Ces indicateurs alimentent la revue annuelle de la politique de gestion des vulnérabilités.**

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