



**MINISTÈRE
DE LA JUSTICE**

*Liberté
Égalité
Fraternité*

**Direction de l'administration
pénitentiaire**

**Maintenance préventive et corrective des
installations de sûreté dans les établissements du
ressort de la Direction Interrégionale des Services
Pénitentiaires Grand-Ouest**

**C.C.T.P. - ANNEXE 08 – AVIS DU CSN (CONSEILLER
SECURITE NUMERIQUE) PORTANT SUR LES MARQUES A
PROHIBER**



DIRECTION
DE L'ADMINISTRATION PÉNITENTIAIRE

Paris le 18 janvier 2023

Avis du Conseiller sécurité numérique auprès du DAP

	Avis n°6
Projet concerné	Dispositifs de vidéosurveillance de marque HIKVISION
Porteurs du projet	SDPS
Résumé succinct du projet/ du besoin	<p>La marque Hikvision équipe l'ensemble des établissements PPP Thémis (Poitiers, Le Mans, Le Havre, Lille Annœullin, Sud Francilien, Nantes) ; des caméras Hikvision ont été / sont en train / vont être installées dans le cadre de l'obligation contractuelle de renouvellement du parc de vidéo surveillance.</p> <p>La marque a également été retenue par l'APIJ pour la SAS de Caen (déjà équipée en Hikvision) et Colmar (commandes réalisées).</p> <p>Or, le 27 septembre 2022, l'ANSSI a fait publier sur le site cybermalveillance.gouv.fr une « Alerte vulnérabilité informatique » impactant des caméras IP Hikvision.</p> <p>Il y est mentionné « <i>qu'une vulnérabilité critique été découverte dans les caméras IP Hikvision (vulnérabilité immatriculée CVE-2021-36260). Elle permet à un attaquant de prendre le contrôle de l'équipement. Les impacts de l'exploitation de cette vulnérabilité par des acteurs malveillants peuvent être de l'espionnage, du vol ou de la destruction d'information, ou encore provoquer l'indisponibilité du service. Selon la configuration de l'installation, la compromission d'une caméra vulnérable pourrait également permettre à un attaquant de se propager sur le réseau informatique auquel elle est reliée.</i> »</p> <p>A titre complémentaire la SDPS a trouvé, en sources ouvertes, les éléments suivants sur cette marque : « Une faille RCE – Remote Code Execution affecte la plupart des caméras de surveillance Hikvision construite à partir de 2016 jusqu'à aujourd'hui (hors caméras patchées après septembre 2021). Les failles RCE sont des vulnérabilités de sécurité logicielle permettant l'exécution d'un code malveillant en local ou à distance vers l'équipement concerné [...] cette faille est exploitable à distance ou en local sans nécessiter la moindre authentification tout en ne laissant aucune trace d'effraction dans les logs, rendant les attaques des plus discrètes... L'équipement concerné pourrait être rendu inutilisable et la compromission des identifiants/mdp est bien sûr, totalement possible. L'autre volet obscur lié à l'existence de ce type de vulnérabilité, réside dans la possibilité de cyberattaque par « rebonds » avec des risques éventuels de compromission du réseau interne qui pourrait faciliter cette méthodologie d'attaque aussi connue sous l'appellation « d' Island Hopping ». Des attaques qui pourraient s'appuyer sur une caméra de vidéoprotection vulnérable telle une Hikvision non patchée, en tant que passerelle vers les infrastructures informatiques d'un fournisseur tiers » (mail du 17/01/2023 de P. Blosseville).</p>

DAP

Adresse postale : 13, place Vendôme - 75042 PARIS Cedex 01
Bureaux situés : 8 - 10, rue du renard - 75004 PARIS
Tél. : 01 49 96 27 16

Risques SSI identifiés	<p>Les audits réalisés récemment par l'ANSSI mais aussi ceux réalisés par des sociétés labellisées par l'ANSSI sur plusieurs structures laissent à penser que les problèmes de cloisonnement du réseau de vidéo protection de la DAP sont exploitables dans le cadre d'attaques telles que décrites ci-dessus.</p> <p>Seul l'inventaire complet (incluant dossiers d'architecture et la matrice des flux détaillés) sollicité par note DAP du 23/12/2022 permettra de confirmer ou d'infirmer cette vulnérabilité.</p>
Avis du CSN	<p>La mise à jour du micro-logiciel des caméras Hikvision déjà installées ou seulement commandées – même si les contraintes opérationnelles liées à cette Màj ne sont pas clairement connues (Màj centralisée par établissement ou caméra par caméra) – est potentiellement susceptible de répondre aux vulnérabilités identifiées.</p> <p>Néanmoins, compte tenu de la nature des risques et de la probabilité de leur survenance, dans la mesure du possible et selon la criticité des structures ou de l'avancement des projets concernés, le CSN préconise, dans le cadre de nouveaux marchés de constructions ou de remplacements, de ne plus avoir recours, aux dispositifs de marque Hikvision.</p>
Références éventuelles	Note DAP du 23/12/2022 portant sur l'optimisation de la vidéo-protection.

le conseiller sécurité numérique
auprès du directeur,

Antoine Danel

DAP

Adresse postale : 13, place Vendôme - 75042 PARIS Cedex 01
Bureaux situés : 8 - 10, rue du renard - 75004 PARIS
Tél. : 01 49 96 27 16