Corrigé Activité P1C9

Le processus imaginé par l'équipe de développement repose sur une confiance aveugle envers le réseau de diffusion de contenu (CDN) externe et le réseau Internet en général.

Si le CDN venait à être compromis par des pirates, ou si un attaquant se positionnait sur le réseau d'un client B2B pour intercepter le trafic (Man-in-the-Middle), il pourrait facilement intercepter la requête de mise à jour. L'attaquant n'aurait qu'à renvoyer un fichier malveillant (un cheval de Troie) à l'application cliente. Puisque l'application cliente exécute le fichier dès la fin du téléchargement sans se poser de questions, elle infecterait le serveur du client B2B, détruisant instantanément la réputation de TechNova.

Pour corriger définitivement cette vulnérabilité de la catégorie A08, vous devez inclure l'exigence d'architecture sécurisée suivante dans les spécifications du module client :

"Afin de garantir l'intégrité de la chaîne de distribution logicielle, l'application cliente DOIT vérifier systématiquement la signature numérique cryptographique de tout exécutable ou de toute mise à jour téléchargée. Cette validation doit être effectuée à l'aide de la clé publique officielle de TechNova AVANT de lancer la moindre procédure d'installation. Toute mise à jour dont la signature est absente ou invalide doit être immédiatement rejetée et supprimée."

N'approuvez jamais aveuglément les données sérialisées ou les fichiers exécutables provenant d'une source externe, qu'il s'agisse d'un utilisateur ou d'un serveur tiers de distribution, sans effectuer un contrôle strict de leur authenticité et de leur intégrité via la cryptographie.