PREMIÈRE MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le Directeur général

Paris, le 28 DEC. 2023
N° 2281 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU ELEMENTAIRE

TRACKWATCH
VERSION 2.5.X POUR X ≥ 3

GATEWATCHER

RCS 810 505 248

75, boulevard Haussmann
75008 Paris
France

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;

Vu le processus de qualification d'un produit, version en vigueur ;

Vu le rapport de certification, ANSSI-CC-2023/24, 18/12/2023 ;

Vu le dossier de demande de qualification déposé par GATEWATCHER,

Décide :

Art. 1er – Le produit fourni par la société GATEWATCHER portant le nom « TRACKWATCH » en version 2.5.x pour x ≥ 3 respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 et est qualifié au niveau élémentaire sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 2 – La présente décision est valable jusqu'au 10 juin 2025.

Art. 3 - Cette décision pourra être prolongée de 18 mois supplémentaires après une nouvelle décision de l'ANSSI s'appuyant sur le rapport relatif à l'évaluation de l'efficacité des fonctions de détection par un jeu de tests validé par l'ANSSI. Cette évaluation devra être réalisée avant le 31 décembre 2024 et ne concernera pas la sécurité relative à la sonde déjà évaluée dans le cadre de la Certification de Sécurité de Premier niveau délivrée par le Centre de Certification National.

Art. 4 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Vincent STRUBEL
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Annexe

Conditions et limites de la qualification.

Références

[1]. Rapport de certification, ANSSI-CC-2023/24, 18/12/2023 ;

[2]. Cible de sécurité GATEWATCHER TRACKWATCH, Solution de détection des incidents de sécurité, version IT17 du 11/01/2021 ;

[3]. Référentiel d'exigences relatif aux prestataires de détection des incidents de sécurité disponible sur www.cyber.gouv.fr- version 2 du 21 décembre 2017.

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C0. Elle emploie la version qualifiée du produit la plus à jour.

C1. La sonde est placée en dérivation des flux à analyser et non en coupure.

C2 la dérivation des flux à analyser vers la sonde est réalisée par un TAP qualifié par l'ANSSI au niveau élémentaire.

C3 La sonde est placée au plus près du point de dérivation. Seul un agrégateur de flux respectant les exigences définies dans l'annexe 5 du référentiel [3] peut être déployé entre le TAP et la sonde.

C4 Le réseau sur lequel le système de détection est déployé est en adéquation avec les capacités fonctionnelles du modèle choisi (débit des flux à analyser, capacité de stockage, etc.) et prend en compte la limite L2 (nature des flux à analyser) identifiée ci-dessous.

C5 Les utilisateurs du système de détection sont, selon leur rôle, formés aux composants du système de détection et la documentation de ces composants leur est mise à disposition.

C6 la sonde dispose d'une base des règles de détection à jour conformément au chapitre intitulé « Gestion des incidents » du référentiel [3].

C7 La sonde est déployée selon des lois et règlementation en vigueur, notamment vis-à-vis des types d'informations pouvant être contenus dans les flux à analyser (données à caractère personnel, ...).

C8 Le système d'information du service de détection opérant le système de détection respecte les exigences établies dans le référentiel [3].

C9 La sonde est déployée dans une enclave de collecte respectant les exigences établies dans le chapitre intitulé « Enclave de collecte au sein du système d'information du commanditaire » du référentiel [3].

C10 Les fonctions d'administration à distance offertes nativement par certains matériels constituant la sonde sont désactivées par défaut, dans la version livrée. Elles ne doivent en aucun cas être réactivées par l'administrateur système de la sonde.

C11 Les composants du système de détection sont hébergés dans des locaux sécurisés dont l'accès est contrôlé et restreint à du personnel de confiance.

C12 Lorsqu'un prestataire de détection supervise les systèmes d'information de plusieurs clients, il met en œuvre un centre de gestion et un centre d'exploitation par le client.

C13 Les objectifs de sécurité sur l'environnement définis dans la cible de sécurité [2] (chapitre III) doivent être respectés.

C14. Les restrictions d'usage figurant dans le rapport [1] doivent être respectées.

C15. Les recommandations figurant dans les guides du produit référencés dans l'annexe A du rapport [1] doivent être respectées.

C16. En cas d'utilisation d'un serveur LDAP pour l'authentification à l'application web de Gcenter, le bénéficiaire devra s'assurer du contrôle total de ce serveur.

Limites

L1. Seules les fonctions identifiées dans le rapport [1] sont couvertes par la présente décision de qualification.

L2. La présente décision de qualification ne couvre pas le décodage et l'analyse des protocoles de type industriels par le système de détection.

L3. l'authentification LDAP sur l'application web GCENTER est exclue du périmètre.