Note de Version GCap 2.5.3.103

Gatewatcher

Created on : Janvier, 2021

Last updated : avril, 2021

Table des matières

Chapitre 1

Note de Version GCap 2.5.3.103

Vous trouverez :
- Nouvelles Fonctionnalités.
- Les correctifs.
- Les problèmes connus.

Chapitre 2

Nouvelles fonctionnalités

2.1 Agrégation des interfaces de monitoring

Le système d'agrégation des interfaces de monitoring (clusters d'interfaces) a été revu, afin de le fiabiliser. Il est désormais possible de brancher un GCap sur un TAP haut débit divisant le flux montant et le flux descendant.

Un cluster est constitué d'exactement deux interfaces de monitoring. Ces clusters sont paramétrables grâce aux interfaces de configuration du GCap.

2.2 Règles de détection par interfaces de monitoring et par VLAN (multi-tenancy)

La prise en charge de jeux de règles de détection distincts a été ajoutée. Ces jeux de règles peuvent être appliqués à des interfaces de monitoring ou à des VLAN spécifiques. Cette configuration est effectuée depuis un GCenter compatible (voir les notes de version des GCenter).

Le support de règles de détection par interface est, pour le moment, limité en combinaison avec les clusters d'interfaces.

2.3 Moteur de détection

La procédure de démarrage et d'arrêt du moteur de détection a été revue, afin d'améliorer les contrôles sur l'intégrité de ses composants.

À chaque démarrage, il vérifie la connectivité des interfaces de monitoring reliées au GCap. Il doit avoir au minimum une interface ou un cluster actif pour se lancer. Il vérifie également que les règles de filtrage sont bien appliquées sur les interfaces de monitoring pertinentes.

Les journaux du moteur de détection ont été unifiés, pour plus de simplicité.

Le durcissement du moteur de détection a été effectué, en créant un environnement aux ressources plus contraintes, et aux permissions plus restrictives.

2.4 Commande Line Interface (CLI)

Il est désormais possible de manipuler la configuration du GCap via une interface utilisateur en ligne de commande (CLI).

La CLI devient l'interface de configuration par défaut du GCap pour tous les utilisateurs. Chaque utilisateur peut choisir de remettre l'interface graphique comme son interface par défaut.

Cette interface est adaptative, en fonction de l'état actuel du GCap et des privilèges de l'utilisateur. Cela vise à proposer uniquement à l'utilisateur des commandes pertinentes.

La configuration des règles de détection locale ainsi que le filtrage des paquets (XDP) n'est possible qu'au travers de l'interface graphique.

2.5 Compte utilisateur et Mot de passe

Depuis la version 2.5.3.103 du GCap, il est possible de changer les mots de passe utilisateurs à tout moment, y compris lorsque le moteur de détection est lancé.

Cette modification permet de forcer le changement de mots de passe lors de la première connexion. Cela a également permis l'ajout de la notion d'un âge maximum dans la politique de mots de passe.

Par ailleurs, une durée maximale de connexion à une session a été ajoutée. Passé ce délai, la session est clôturée automatiquement. Cette durée est configurable et optionnelle.

Un avertissement a été inclus quant à l'utilisation du compte 'root', qui invalide le support.

2.6 Niveaux de criticité des journaux applicatifs

La cohérence des niveaux de criticité des journaux applicatifs a été améliorée.

2.7 Bannière SSH préauthentification

Une bannière affichée avant l'authentification SSH peut être configurée sur les GCenter compatibles.

2.8 Éditeur de texte pour la saisie des règles de détection locales

L'interface de saisie des règles de détection locale a été améliorée. Elle s'effectue désormais dans un éditeur de texte plus évolué.

2.9 Durcissement système

Une protection contre la corruption des programmes est désormais mise en place dès le démarrage du GCap.

2.10 Gestion des protocoles et journalisation

Le moteur de détection est désormais capable d'analyser de nouveaux protocoles :

- Kerberos
- DHCP
- TFTP
- IKEv2
- NFS
- NTP

Par défaut, tous ces nouveaux protocoles sont analysés et leurs métadonnées sont journalisées.

La gestion de certains protocoles (FTP, DNS, SMB) a également été améliorée.

Pour des raisons de sécurité, la reconstruction des flux SMB et FTP a été limitée à 10MB.

La gestion des eve-logs DNS a été améliorée.

2.11 Nouveau mode de compatibilité avec le GCenter

Un nouveau mode de compatibilité « GCenter v101+ » a été ajouté au GCap.
Avec ce mode, il est possible de déléguer la configuration des nouveaux protocoles (c.f. *Gestion des protocoles et journalisation*) aux GCenter en version 2.5.3.101 ou supérieure.
Dans les autres modes de compatibilité possibles, l'activation/désactivation de ces nouveaux protocoles se fait au travers des interfaces de configuration du GCap.

2.12 Rejouer un flux au format PCAP

Il est possible de rejouer un flux au format PCAP. Cela permet d'émuler un trafic réseau, afin d'effectuer des tests fonctionnels de la sonde.
Cette fonctionnalité est activable uniquement en combinaison avec un GCenter compatible.

2.13 Amélioration de la journalisation système

Les journaux système ont été étoffés d'information sur le succès et l'échec du transfert de fichiers vers le GCenter.

2.14 Protection bruteforce

Une protection contre le bruteforce de mots de passe par SSH a été ajoutée au GCap. Il est possible de configurer le nombre de tentatives et la durée de verrouillage.

2.15 Préfiltrage des eve-log

Les évènements de type fileinfo pour les fichiers non conservés pour analyse ultérieure peuvent désormais être éliminés par le GCap. Cela évite de surcharger le GCenter avec des informations potentiellement jugées inutiles.
Ce préfiltrage peut être activé ou désactivé.

2.16 Compression des journaux

Il est désormais possible de compresser les journaux en attente d'envoi au GCenter. Il est conseillé d'activer cette fonctionnalité en cas de connectivité intermittente, ou tout autre problème prévenant l'envoi des journaux au GCenter.
Elle est désactivée par défaut pour des raisons de performances.

2.17 Réduction de la surface d'attaque sur le GCap

Le composant logiciel sécurisant les applications en conteneurs a été remplacé par un utilitaire plus léger et plus configurable. Cela permet de réduire la surface d'attaque et d'affiner les contrôles de sécurité effectués sur les conteneurs.

2.18 GCap 1000 series

La version 2.5.3.103 prend en charge les GCaps 1000 series.

Chapitre 3

Correctifs

3.1 Mise à jour du moteur de détection

Le moteur de détection a été mis à jour afin d'intégrer les correctifs de l'éditeur de la solution open source.

3.2 Mise à jour système des conteneurs

Certaines applications sensibles constituant le GCap sont placées dans des conteneurs système. Ces derniers ont été mis à jour afin d'intégrer les derniers correctifs de sécurité.

3.3 Reconfiguration du moteur de détection

Pendant la reconfiguration du moteur de détection, il y avait trop d'informations journalisées. Les actions journalisées sont désormais plus nombreuses et les informations plus cohérentes.

3.4 Rafraichissement du statut des interfaces

Le bouton rafraichir du menu « Interfaces » rafraichit désormais correctement le statut des interfaces.

3.5 Configuration de la politique de mot de passe

Il était possible de configurer une politique de mot de passe avec des valeurs négatives ou beaucoup trop grandes. Des valeurs minimum et maximum ont été définies.

3.6 Correction des conditions de démarrage et d'arrêt des services

Au redémarrage d'un GCap, suite à une coupure de courant, certains services refusaient de se lancer, détectant qu'ils l'étaient déjà. La gestion des fichiers temporaires a été corrigée pour éviter cette situation lors de redémarrages inopinés.
La séquence de démarrage du moteur de détection était également incorrecte. Suite à un démarrage où une erreur survenait, le moteur démarrait spontanément à la résolution de l'erreur au lieu de démarrer à la demande.

3.7 Fonction de RESET

La fonction 'reset' a été supprimée.

3.8 Durcissement de la configuration réseau de routage

La configuration réseau était altérée automatiquement par un service système. Cette modification affaiblissait les règles de routage durcies qui avaient été établies.
L'état précédent n'avait pas d'impact significatif puisque si des flux étaient routés à cause de la configuration laxiste, ils étaient stoppés par le pare-feu.
Le service système responsable de la configuration laxiste a été remplacé par une version moins intrusive, et le routage est désormais correctement durci.

3.9 Message d'erreur 'inattendu'

Lors de l'arrêt du moteur de détection, les journaux enregistraient un message d'erreur inexact. Le message rapportait une erreur « inattendue et exceptionnelle » alors qu'elle était « attendue et tolérable ».

3.10 Arrêt du service de synchronisation

L'arrêt inopiné du service de synchronisation des fichiers de règles et de configuration entre un GCap et le GCenter pouvait survenir. Le problème était dû à de multiples tentatives simultanées d'effacement d'un même fichier temporaire. La logique de suppression a été améliorée.
L'arrêt inopiné pouvait également survenir lors de problèmes de connectivité ou lorsque des fichiers provoquaient une erreur dans la bibliothèque d'inférence de types de fichiers.
En outre, ce service pouvait parfois mettre trop de temps à s'arrêter, notamment pendant le changement de la configuration réseau. Une optimisation du service a été effectuée pour raccourcir ce délai.

3.11 Envoi de fichiers extraits

Le délai de grâce avant de déclarer impossible le transfert de fichiers extraits entre un GCap et un GCenter a été allongé. Ce changement permet d'améliorer la compatibilité avec les réseaux à connectivités limitées.

3.12 Noms des interfaces réseau

La génération des noms des interfaces réseau pouvait être fausse suite à des cas exceptionnels comme le branchement de SPF non reconnus par les drivers réseau du kernel.
La gestion a été refaite pour corriger ce problème.

3.13 Génération d'évènements de type fileinfo

Les évènements de type fileinfo étaient toujours générés, même lorsque l'extraction de fichiers était désactivée. La génération de trafic était incohérente par rapport à la configuration demandée.

3.14 Journaux netdata

Il est possible de voir les journaux netdata depuis le menu « inspect ».

3.15 Extraction par extension de fichier

Les extensions à extraire, définies depuis l'interface web du GCenter, sont maintenant extraites par le GCap.

Chapitre 4

Problèmes connus

4.1 Transactions TCP et fichiers extraits

Toutes les versions de Suricata (4.X, 5.X, et 6.X) comportent un bug rapportant de manière erronée qu'un fichier extrait et d'intérêt n'a pas été extrait. Le problème apparaît pour les sessions TCP se déroulants de la manière suivante :

— Initial handshake.
— PUSH d'un fichier dans son intégralité sans aucun ACK.
— ACK de l'ensemble des segments et fermeture de la connexion par RST.

Ce rapport erroné perturbe le fonctionnement du GCap qui n'envoie pas le fichier au GCenter.

Un correctif partiel est présent dans les versions supérieures ou égales à 2.5.3.104.

4.2 Remise à zéro du GCap

La fonction reset n'est pas assez fiable dans les GCap de version égale ou supérieur à 2.5.3.103, et a été désactivée. Son fonctionnement sera revu et corrigé dans son intégralité dans la version 2.5.3.105.

4.3 Affichage erroné du statut des interfaces de monitoring

Lorsque la carte réseau est défaillante, le statut de l'interface concernée affiché par l'utilitaire de configuration peut être erroné.

4.4 Rejeu des fichiers PCAPs

La fonction « replay pcap » n'est pas opérationnelle lorsque le multi-tenancy par interface est employé.

4.5 Protection du mécanisme d'authentification (anti-bruteforce)

Le compteur de tentatives d'authentification est incrémenté dès qu'une tentative d'ouverture de session a lieu, même si aucun mot de passe n'est entré par l'utilisateur.