Note de Version GCap 2.5.3.104

Gatewatcher

Created on : Mars, 2021

Last updated : avril, 2021

Table des matières

Chapitre 1

Note de Version GCap 2.5.3.104

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

Chapitre 2

Correctifs

2.1 Correction de la répartition de la charge de travail de Suricata

Certains CPU n'étaient pas employés à leur plein potentiel. Ce bug était dû à la technologie de conteneurisation LXC qui prenait sur elle d'effectuer une altération inattendue et indésirable du système. Cette altération a été retirée du code de LXC, et l'équilibrage rétabli.

2.2 Corruption de la détection de flux légitimes

Suricata 4.1.6 contenait un patch de l'éditeur lié à la CVE-2019-18625 pour prévenir certaines techniques de contournement de la détection.

En raison de ce patch, certains flux légitimes n'étaient pas détectés.

Nous avons désactivé celui-ci pour restaurer la détection correcte de ces flux.

Les versions 2.5.3.101 et antérieures n'étaient pas affectées par ce bug.

2.3 Correction d'un problème de reconnaissance de certains formats de fichiers .zip

Depuis la version v2.5.3.102, un bug avait été introduit pour la détection de certains fichiers .zip. Celui-ci était lié à une optimisation excessive des performances. Ce correctif permet la détection correcte de tous les fichiers .zip, sans sacrifier les performances.

2.4 Problème d'extraction de fichiers lors de certaines transactions TCP

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.

Dans l'attente d'un correctif officiel, nous avons compensé ce souci par le développement d'un correctif partiel qui envoie tout de même les fichiers au GCenter ne perturbant plus le fonctionnement du GCap. Ce correctif ne peut cependant retrouver les métadonnées associées aux fichiers concernés par ce bug. Les métadonnées rapportées pour ces fichiers sont donc fausses, nous les avons fixées à des valeurs reconnaissables :

— **127.0.0.1** pour l'adresse IP source et de destination.
— **12345** pour le port TCP source et de destination.
— Protocole de transport **http**.

Le correctif ajouté est déclenché périodiquement toutes les 15 minutes et introduit donc une latence entre le moment où les fichiers sont extraits sur le GCap et le moment où ils sont envoyés au GCenter.

2.5 Correction d'un problème de stabilité du démon de mise à jour des règles

Le démon en charge de la mise à jour des règles pouvait s'arrêter inopinément lorsque la connectivité avec le GCenter était perdue. Cette erreur avait une très faible probabilité de survenir et était présente depuis la version 2.5.3.2. Le correctif s'assure que la condition de survenue de l'erreur soit mieux encadrée pour ne plus provoquer l'arrêt inopiné, et journaliser l'événement.

2.6 Correction de la génération des règles de reconstruction de fichiers lors de l'utilisation de cluster d'interface en mode multi-tenant

Lorsque des cluster d'interfaces étaient employés, en combinaison avec l'utilisation de detection ruleset de type multi-tenant, un problème pouvait survenir dans la génération des règles relatives à la reconstruction de fichier. Cela pouvait rendre la reconstruction de fichier inopérante dans ce cas précis.

Chapitre 3

Problèmes connus

3.1 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.

3.2 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.

3.3 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.

3.4 Rejeu des fichiers PCAPs

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

3.5 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.