STORMSHIELD ENDPOINT SECURITY EVOLUTION

NOTES DE VERSION

Version 2

Dernière mise à jour du document : 17 décembre 2020

Référence : ses-fr-notes_de_version-v2.0.1

Table des matières

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Vulnérabilités résolues de SES Evolution 2.0.1

Ajout d'une protection contre les attaques par déni de service

Une protection anti DDoS a été ajoutée sur l'API qui enregistre un nouveau gestionnaire d'agents dans le Backend. Désormais un seul gestionnaire d'agents peut être enregistré toutes les 15 secondes.

Suppression d'une valeur dans la base de registre

Une valeur liée à la sécurité des challenges était présente inutilement dans la base de registre. Cette vulnérabilité a été résolue par la suppression de cette valeur.

Correctifs de SES Evolution 2.0.1

Installation de SES Evolution

Champs mots de passe

Dans le Centre d'installation, les champs des mots de passe et leur confirmation sont désormais correctement vérifiés dans tous les cas.

Validité de la licence

Dans le Centre d'installation, le format et la validité de la licence sont vérifiés dès la sélection du fichier de licence et non plus à la fin de l'installation.

Politiques de sécurité

Référence support : 177214CW

Accès réseau

Il est maintenant possible de bloquer certains accès réseau qui n'étaient pas filtrés par les protections applicatives car effectués par le système. Ceci permet par exemple de bloquer les accès distants à un dossier partagé situé sur une machine protégée par l'agent SES Evolution.

En cas de mise à jour vers SES Evolution 2.0.1, la politique par défaut n'est pas mise à jour. Vous pouvez télécharger le jeu de règles correspondant sur votre espace personnel MyStormshield afin d'ajouter les autorisations d'accès réseau pour les processus système. Pour plus d'informations, reportez-vous à la Base de connaissance Stormshield.

Identifiants réseau

L'option **Inverser la portée de l'identifiant** dans l'édition des identifiants réseaux est désormais sauvegardée correctement.

Règles d'audit sur les pilotes

Les comportements spécifiques des règles de protection Chargement des pilotes et Intégrité des pilotes sont désormais bien appliqués. Ces règles ne génèrent plus de logs injustifiés pour les pilotes autorisés.

Logs

Recherche dans les logs agent

Dans la console d'administration, le délai maximum d'une recherche dans les logs agents est passé de 30 secondes à 15 minutes. Un message est désormais affiché lorsque la recherche dépasse ce délai.

Affichage des incidents

A l'ouverture d'un incident, seuls les logs de type alerte sont désormais affichés, dans la limite de 1000 logs. Le reste des logs est chargé lors de la consultation du graphique d'attaque dans la limite de 100000 logs. Ceci permet de construire le graphique d'attaque avec des logs complets.

Agent SES Evolution

Déploiement des politiques

Les logs très longs ne provoquent plus la fermeture inopinée de l'interface graphique de l'Agent SES Evolution.

Règles d'autoprotection

Les règles d'autoprotection sur certaines clés de registre d'un agent SES Evolution n'étaient pas appliquées correctement. Ce problème a été corrigé.

Affichage

Agents Windows 10

Le panneau **Agents** de la console d'administration affiche désormais la version correcte du système d'exploitation pour les agents Windows 10.

Versions de Microsoft Windows compatibles

SES Evolution version 2 est compatible avec les versions de Microsoft Windows suivantes. Pour plus d'informations, reportez-vous à la section Prérequis système pour SES Evolution du *Guide d'installation*.

Console d'administration
Windows 7 - 32 et 64 bits
Windows 8.1 update - Août 2014 - 32 et 64 bits
Windows 10 Enterprise 2015 LTSB – 32 et 64 bits Windows 10 Enterprise 2016 LTSB – 32 et 64 bits Windows 10 1809 – 32 et 64 bits Windows 10 1909 – 32 et 64 bits Windows 10 2004 – 32 et 64 bits
Windows Server 2008 R2
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Backend
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Gestionnaire d'agents
Windows 10 Enterprise 2015 LTSB – 64 bits Windows 10 Enterprise 2016 LTSB – 64 bits Windows 10 1809 – 64 bits Windows 10 1909 – 64 bits Windows 10 2004 – 64 bits
Windows Server 2008 R2*
Windows Server 2012 R2*
Windows Server 2016
Windows Server 2019

* Sur ces systèmes d'exploitation fraîchement installés, l'installation préalable du framework .NET 4.6.2 est nécessaire pour que le Centre d'installation SES Evolution fonctionne.

Agent
Windows 7 - 32 et 64 bits
Windows 8.1 mise à jour 3 (août 2014) - 32 bits ou 64 bits
Windows 10 Enterprise 2015 LTSB – 32 et 64 bits Windows 10 Enterprise 2016 LTSB – 32 et 64 bits Windows 10 1809 – 32 et 64 bits Windows 10 1909 – 32 et 64 bits Windows 10 2004 – 32 et 64 bits Windows 10 20H2 – 32 et 64 bits
Windows Server 2008 R2
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SES Evolution est consultable sur la Base de connaissance Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissance, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Précisions sur les cas d'utilisation

Installation de la solution SES Evolution

Si une mise à jour Windows est en cours lors d'une installation complète du serveur SES Evolution ou du composant backend, l'installation échoue. Il est recommandé de désactiver les mises à jour Windows avant d'installer SES Evolution et de les réactiver ensuite.

Périphériques Bluetooth Low Energy

Les périphériques Bluetooth Low Energy ne sont pas filtrés par l'agent SES Evolution : seuls les périphériques Bluetooth standard sont reconnus.

Compatibilité avec les autres firewalls

Dans certains cas, lorsqu'un autre firewall avec une priorité supérieure à l'agent SES Evolution est installé sur le même poste de travail et met en attente le traitement d'un paquet, quelle que soit la décision qu'il prendra pour le traiter, SES Evolution n'analysera jamais ce même paquet.

Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de Documentation Technique Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Guide d'installation
- Guide d'administration

Merci de consulter la Base de connaissances (anglais uniquement) pour des informations techniques spécifiques.

Versions précédentes de SES Evolution v2

Retrouvez dans cette section les nouvelles fonctionnalités et correctifs des versions précédentes de SES Evolution v2.

2.0.0	Nouvelles fonctionnalités

Résumé des fonctionnalités

La version 2.0 de SES Evolution offre les fonctionnalités suivantes.

Fonctionnalités de SES Evolution 2.0

Protections	
Contre les débordements mémoire	Protégez votre parc contre des tentatives d'intrusion et des exploitations de vulnérabilités.
Contre la dissimulation de processus	
Contre le vol de jetons de sécurité	
Contre les contournements du système de fichiers	
Contre les enregistreurs de frappes	
Contrôle des accès aux fichiers	Contrôlez l'ensemble des ressources système et des accès qui y sont faits. Autorisez des applications à opérer des changements ou à accéder à ces ressources ou bloquez-les. Vous pouvez également simplement les surveiller.
Contrôle des accès à la base de registre	
Contrôle des accès à la mémoire	
Contrôle des exécutions	
Détection de chargement de pilotes	Détectez les rootkits tentant de charger ou de modifier des pilotes dans le noyau.
Détection d'altération de pilotes	
Pare-feu applicatif	Contrôlez les communications réseau entrantes et sortantes par application.
Contrôle des points d'accès Wi-Fi	Gérez les réseaux Wi-Fi autorisés et empêchez le bridge Wi-Fi-LAN.
Contrôle des lecteurs de disquettes, lecteurs CD/DVD, Ports série	Contrôlez les périphériques autorisés sur votre parc via des règles totalement personnalisables.
Contrôle des périphériques Bluetooth	
Contrôle des périphériques USB	
Sas de décontamination USB	Contrôlez les clés et disques durs USB sur votre parc, gérez les périphériques de confiance et bloquez les périphériques dont le contenu n'a pas été validé.

Paramétrage	
Gestion par groupes d'agents	Organisez votre parc selon vos besoins via un système de groupes d'agents simple et puissant.
Déploiement de configurations	Déployez les nouvelles configurations sur l'ensemble des agents en un clic depuis la console d'administration.
Politique de sécurité Stormshield	Protégez votre parc avec une politique par défaut couvrant les menaces courantes et ajoutez des règles de sécurité personnalisées pour une adaptation totale à votre environnement.

Politiques de sécurité contextuelles	Adaptez la sécurité à l'environnement des agents afin qu'ils appliquent des politiques différentes en fonction de leur emplacement.
Gestion de politiques par jeux de règles	Mutualisez les règles de sécurité dans vos politiques et gérez simplement vos exceptions.
Tâches planifiées	Exécutez des commandes sur les agents en paramétrant des scripts depuis la console d'administration.
Modularité des agents	Gérez les fonctionnalités installées sur chaque agent depuis la console d'administration : désinstallez les fonctionnalités inutiles, supprimez des incompatibilités et limitez la surface d'attaque.
Challenges	Autorisez certaines opérations sur les agents de manière sécurisée via un système de question/réponse.
Connexion simultanée des administrateurs à la console	Organisez vos administrateurs par rôle pour gérer des accès simultanés aux diverses ressources de la console d'administration.

Surveillance de l'activité	
Tableau de bord	Visualisez rapidement l'état de votre parc grâce à un tableau de bord simple.
Suivi des logs	Visualisez les événements produits par les agents en les filtrant par priorité, type, groupe etc.
Analyse d'attaques	Suivez les incidents et analysez les attaques grâce au panneau dédié permettant de revoir graphiquement les étapes et de chercher plus d'informations pour comprendre chaque attaque.
Surveillance des agents	Suivez en temps réel les agents du parc, vérifiez leur état et assignez-les à des groupes.
Export vers un serveur Syslog	Exportez l'ensemble des événements dans votre SIEM pour les intégrer à vos autres sources d'informations de sécurité (firewall, antivirus, etc.).

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Rapporter un incident/Suivre un incident**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.