STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSO AGENT

NOTES DE VERSION

Version 3

Dernière mise à jour du document : 4 mai 2021

Référence : sns-fr-agent_sso_notes_de_version-v3.0.1

Table des matières

Dans la documentation, Stormshield Network Security est désigné sous la forme abrégée : SNS et Stormshield Network sous la forme abrégée : SN.

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

Vulnérabilités résolues de SN SSO Agent 3.0.1

OpenSSL

Une vulnérabilité d'un score global CVSS de 4.0 a été corrigée par la mise à jour du composant OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Compatibilité

Les plate-formes suivantes sont compatibles avec SN SSO Agent 3.0.1 :

Systèmes Windows

Stormshield Network Firewall	Annuaires Active Directory
Versions 4.2 et supérieures	Windows Server 2012 R2, 2016 et 2019

NOTES

- SN SSO Agent pour Windows est un service 32 bits, compatible avec les systèmes d'exploitation 64 bits.
- Si SN SSO Agent dans une version antérieure à la version 1.4 a été installé au préalable, il est impératif de désinstaller le service avant de procéder à l'installation de SN SSO Agent.

Systèmes Linux

Stormshield Network Firewall	Système d'exploitation
Versions 4.2 et supérieures	Ubuntu 18.04 LTS

NOTE

SN SSO Agent pour Linux est un service compatible uniquement avec les systèmes d'exploitation 64 bits.

Précisions sur les cas d'utilisation

Authentification

Si un utilisateur identifié par SN SSO Agent utilise un autre identifiant du domaine sur son poste de travail, cela peut annuler son identification sur le firewall. En effet, cette seconde identification est relayée par le contrôleur du domaine qui remplace la session initiale. Ces cas se présentent notamment pour les accès suivants :

- Connexion sur un intranet avec la méthode *kerberos* et/ou *ntlm*,
- Montage de ressources partagées distantes (fichiers, imprimantes) via le protocole SMB,
- Connexion RDP Terminal Services sur un serveur distant.

Syslog

Les échanges avec le serveur Syslog doivent s'effectuer en UDP. Ce protocole n'offrant aucune garantie de confidentialité ni d'intégrité, nous vous recommandons de sécuriser les échanges entre votre annuaire non Windows (par exemple Samba 4) et votre serveur Syslog afin d'écarter un risque potentiel de sécurité (usurpation d'adresse IP, injection de messages Syslog non autorisés vers votre firewall, etc.).

Sécurisez ces échanges par le biais d'une segmentation du réseau physique ou par VLAN, via un tunnel IPsec, SSH ou SSL, ou encore en positionnant en relai un serveur Syslog TLS entre les deux machines concernées.

Documentation

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

Guide

- Stormshield Network Firewall - Manuel d'utilisation et de configuration

Note technique

- Installation et déploiement SSO Agent pour Windows
- Installation et déploiement SSO Agent pour Linux

Merci de consulter la Base de connaissance Stormshield pour obtenir des informations techniques spécifiques et pour accéder aux vidéos créées par l'équipe du support technique (Technical Assistance Center).

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 3.0.1 de SN SSO Agent :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires SN SSO Agent :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur l'espace client MyStormshield, rubrique Téléchargements.

Versions précédentes de SN SSO Agent 3

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SN SSO Agent 2.

3.0.0	Fonctionnalités	Correctifs

Nouvelles fonctionnalités de SN SSO Agent 3.0.0

Authentification

SN SSO Agent prend désormais en charge le protocole TLS v1.2 lors de l'établissement d'une connexion au service d'authentification du firewall.

Toutes les versions SNS ne prennent pas en charge le protocole TLS v1.2. Veuillez-vous reporter à la section **Compatibilité** pour plus d'informations.

Installation sous Windows

Initialement proposé sous forme d'exécutable, SN SSO Agent pour Windows est désormais uniquement disponible en tant que package MSI (Microsoft System Installer). Ceci lui permet toujours d'être déployé localement mais aussi via une GPO (Group Policy Object) dans un domaine Microsoft Active Directory.

Correctifs de SN SSO Agent 3.0.0

Système

Microsoft Windows Server 2016

Référence support 77539

Les bibliothèques Microsoft vcruntime140.dll et msvcp140.dll ont été ajoutées au programme d'installation de SN SSO Agent.

Décalage d'heure d'événement / Agent SSO

Référence support 78457

Lorsqu'un événement d'authentification survenait avec une date plus récente que l'heure de la machine hébergeant SN SSO Agent, l'authentification de l'utilisateur concernée était refusée. Cette anomalie a été corrigée.

Détection des déconnexions par PING

Référence support 78379

L'activation de la méthode de détection des déconnexions par PING ne provoque plus de blocage inopiné de SN SSO Agent.

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/.