STORMSHIELD

# STORMSHIELD NETWORK SECURITY

## STORMSHIELD NETWORK SSO AGENT

# NOTES DE VERSION

Version 2

Dernière mise à jour du document : 24 mai 2022

Référence : sns-fr-agent_sso_notes_de_version-v2.1.1

# Table des matières

Vulnérabilités résolues de la version 2.1.1 ..... 3
Compatibilité ..... 4
Précisions sur les cas d'utilisation ..... 5
Ressources documentaires ..... 6
Télécharger cette version ..... 7
Versions précédentes de SN SSO Agent 2 ..... 8
Contact ..... 12

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

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

# Vulnérabilités résolues de la version 2.1.1

## Installation

Une vulnérabilité de sévérité moyenne dans le mécanisme d'installation de SN SSO Agent a été corrigée.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-001/.

# Compatibilité

Les plate-formes suivantes sont compatibles avec SN SSO Agent 2.1.1.

## Systèmes Windows

| Stormshield Network Firewall | Annuaires Active Directory |
|---|---|
| 2.7, 3.x, 4.0 et 4.1 | Windows Server 2012 R2, 2016, 2019 et 2022 |

**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 |
|---|---|
| 3.10, 3.11 LTSB et 4.1 | Ubuntu 18.04 LTS 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.

# Ressources documentaires

Les ressources documentaires techniques 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.

Merci de consulter la Base de connaissances 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 2.1.1 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 2

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

| | | |
|---|---|---|
| 2.1.0 | | Correctifs |
| 2.0.0 | Nouvelles fonctionnalités | Correctifs |

# Correctifs de la version 2.1.0

## 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.

# Nouvelles fonctionnalités de la version 2.0.0

## Authentification

### Nouvel SN SSO Agent pour Linux

Un nouvel SN SSO Agent est disponible sous Linux et supporte les annuaires non Windows (par exemple Samba 4). Sa configuration s'effectue dans le module **Authentification** de l'interface web d'administration et la détection au travers de logs exportés via Syslog. Les logs exportés sont filtrés selon des expressions régulières configurées dans l'interface.

**NOTE**
Les versions 4.0.x des firewalls SNS ne sont pas compatibles avec le SN SSO Agent pour Linux.

# Correctifs de la version 2.0.0

## Système

### Microsoft Active Directory

**Référence support 74708**

Un risque de fuite mémoire lors d'une erreur de connexion vers un annuaire Microsoft Active Directory a été corrigé.

# Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/

La soumission d'une requête auprès du support technique doit se faire par le biais du gestionnaire d'incidents présent dans l'espace client MyStormshield, menu **Support technique** > **Rapporter un incident / Suivre un incident**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace client MyStormshield.

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

*Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*