STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

NOTES DE VERSION

Version 3

Dernière mise à jour du document : 23 février 2023

Référence : sns-fr-ssl_vpn_client-notes_de_version-v3.2.1

Table des matières

Dans la documentation, Stormshield Network SSL VPN Client est désigné sous la forme abrégée : SN SSL VPN Client 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.

Compatibilité

Les plate-formes suivantes sont compatibles avec SN SSL VPN Client 3.2.1.

Stormshield Network Firewall

3.x et 4.x

Systèmes d'exploitation

Windows 8.1 64 bits
Windows 10 64 bits (à jour)
Windows 11 64 bits

> **NOTE**
> SN SSL VPN Client n'est pas compatible avec les ordinateurs, téléphones et tablettes équipés d'un processeur ARM.

Méthodes d'authentification multifacteur

Ce tableau récapitule les méthodes d'authentification multifacteur compatibles selon la version installée sur le firewall SNS et le mode de connexion utilisé par **SN SSL VPN Client**.

Version SNS	Mode de connexion utilisé par SN SSL VPN Client	Mot de passe + Code OTP	Code OTP seulement	Mode Push	TOTP
4.5 ou supérieure	Tous les modes	✓	✓	✓	✓
4.3, 4.4	Tous les modes	✓	✓	✓	✗
3.x, 4.2 ou inférieure	Mode Automatique	✗	✗	✗	✗
	Mode Manuel	✓	✓	✗	✗

Les modes de connexion de SN SSL VPN Client sont : Mode Automatique et le Mode Manuel.

Vulnérabilités résolues de la version 3.2.1

OpenSSL

Une vulnérabilité de sévérité moyenne a été corrigée dans OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2023-011.

Correctifs de la version 3.2.1

Authentification multifacteur - OTP

Référence support 85005

Un problème empêchant l'authentification avec un code OTP a été corrigé. Cette régression était apparue en version SN SSL VPN Client 3.2.0.

Scripts *.bat* exécutés par SN SSL VPN Client

Interruption du tunnel VPN après l'exécution d'un script d'ouverture

Référence support 85009

L'exécution d'un script par SN SSL VPN Client à l'ouverture du tunnel VPN avec le firewall SNS interrompait le tunnel si l'exécution du script durait deux secondes ou plus. Ce problème, qui générait l'erreur "*La connexion VPN SSL a été interrompue pendant la mise en veille ou la veille prolongée de Windows. Merci de vous reconnecter.*", a été corrigé.

Suppression des scripts d'ouverture et de fermeture

Référence support 85013

Les scripts exécutés par SN SSL VPN Client à l'ouverture et à la fermeture du tunnel VPN avec le firewall SNS n'étaient pas supprimés du poste de travail Windows lorsqu'ils avaient été retirés de la configuration VPN SSL du firewall SNS. Ces scripts continuaient donc de s'exécuter. Ce problème a été corrigé.

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 3.2.1 de SN SSL VPN Client :

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 SSL VPN Client :

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 SSL VPN Client 3

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes de SN SSL VPN Client 3.

3.2.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.1.1			Correctifs
3.1.0		Vulnérabilités résolues	Correctifs
3.0.1			Correctifs
3.0.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs

Nouvelles fonctionnalités et améliorations de la version 3.2.0

Installation

La version SN SSL VPN Client 3.2 introduit la possibilité d'installer SN SSL VPN Client sur une machine sans devoir désinstaller au préalable la version d'origine, tant que cette dernière est égale ou supérieure à la version 2.9.

Vulnérabilités résolues de la version 3.2.0

Système

Une vulnérabilité de sévérité forte a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-028/.

Des vulnérabilités de sévérité moyenne ont été corrigées dans SN SSL VPN Client.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2022-028/,
- https://advisories.stormshield.eu/2022-029/.

Correctifs de la version 3.2.0

Utilisation sur un profil utilisateur Windows avec des caractères spéciaux

Référence support 84668

SN SSL VPN Client fonctionne désormais correctement lorsqu'il est installé sur un profil utilisateur Windows dont le nom d'utilisateur contient des caractères spéciaux (é, ç, ę, ć, ...). Ce problème générait l'erreur "*Échec de l'extraction du fichier de configuration*".

Sortie du mode veille ou de la veille prolongée d'une machine Windows

Référence support 84499

Si le VPN n'était pas déconnecté et que la machine Windows entrait en veille ou veille prolongée, les routes incluses dans la configuration VPN SSL et installées sur le poste n'étaient pas supprimées. Ceci pouvait empêcher le tunnel VPN de fonctionner après la sortie du mode veille ou de la veille prolongée.

Ce comportement a été corrigé et le tunnel VPN est désormais déconnecté automatiquement après la sortie du mode veille ou de la veille prolongée. L'utilisateur en est informé par l'affichage d'une notification.

Correctifs de la version 3.1.1

Système

Installation

Référence support 84687

Un problème empêchant l'installation du SN SSL VPN Client en version 3.1.0 lorsque le pilote réseau TAP était déjà installé sur le système a été corrigé. Ce problème générait l'erreur "*Ce paquet Windows Installer rencontre un problème.*".

Désinstallation

Un problème empêchant la désinstallation du SN SSL VPN Client en version 3.1.0 lorsque le pilote réseau TAP n'était plus présent sur le système a été corrigé.

Vulnérabilités résolues de la version 3.1.0

Système

Une vulnérabilité de sévérité forte a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-004/.

Correctifs de la version 3.1.0

Système

Établissement d'un tunnel

Référence support 82807

Un problème empêchant l'établissement d'un tunnel VPN SSL lorsque des paramètres de proxy étaient configurés dans les propriétés d'Internet Explorer a été corrigé. Cette régression était apparue en version SN SSL VPN Client 2.9.1.

Correctifs de la version 3.0.1

Système

Mode automatique - Saisie d'un port personnalisé

Référence support 84329

En mode automatique, la saisie d'un port personnalisé utilisé pour le portail captif (différent du port par défaut 443) est désormais correctement prise en compte par SN SSL VPN Client.

Fichier *auth_management.txt* manquant après installation du SN SSL VPN Client

Référence support 84348

Dans certaines configurations, même si l'installation du SN SSL VPN Client arrivait à son terme, le fichier *auth_management.txt* n'était pas installé sur le système empêchant alors SN SSL VPN Client de fonctionner. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de la version 3.0.0

Compatibilité

SN SSL VPN Client en version 3.0.0 est désormais un service 64 bits. Il devient donc uniquement compatible avec les systèmes d'exploitation 64 bits.

Authentification multifacteur - OTP

Un utilisateur peut désormais spécifier qu'il utilise une authentification multifacteur en cochant une nouvelle option sur la fenêtre de connexion du SN SSL VPN Client en version 3.0.0. En cochant l'option, l'utilisateur peut alors renseigner un Code OTP dans un champ distinct.

Cet ajout permet au SN SSL VPN Client de supporter les méthodes d'authentification multifacteur suivantes :

- **Mot de passe + Code OTP** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée et les champs **Mot de passe** et **Code OTP** doivent être complétés,
- **Code OTP seulement** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée, le champ **Mot de passe** doit être laissé vide et le champ **Code OTP** doit être complété,
- **Mode Push** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée et les champs **Mot de passe** et **Code OTP** doivent être laissés vides.

Pour plus d'informations sur la compatibilité des méthodes d'authentification multifacteur selon la version installée sur le firewall SNS et le mode de connexion utilisé par SN SSL VPN Client, reportez-vous à la section Compatibilité.

Plus d'information sur la configuration et l'utilisation du VPN SSL des firewalls SNS.

Vulnérabilités résolues de la version 3.0.0

Système

Une vulnérabilité de sévérité moyenne a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-019/.

Correctifs de la version 3.0.0

Système

Déconnexion du tunnel à la fermeture de session

Références support 81985 - 82934 - 83152

Lorsqu'un utilisateur fermait puis rouvrait sa session Windows sans redémarrer sa machine, SN SSL VPN Client ne déconnectait pas le tunnel à la fermeture de la session Windows. Le tunnel était ainsi toujours monté à la réouverture de la session Windows malgré le fait que l'icône du SN SSL VPN Client dans la barre des tâches indiquait le contraire. Ce problème a été corrigé.

Déploiement avec Microsoft Intune

Référence support 82577

SN SSL VPN Client en version 2.9 n'était pas fonctionnel après avoir été déployé avec Microsoft Intune. Ce problème 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.