Waterfall Security Solutions Ltd.

Cible de sécurité CSPN

WF-502F

Tableau des révisions

Révision	Date	Auteur	Commentaires
0.1	30/11/2015	SERMA	Version initiale
1.0	18/01/2016	SERMA	Prise en considération de la première révi-sion
1.1	04/02/2016	SERMA	Prise en considération des commentaires d'Oppida
1.2	02/03/2017	Waterfall	Prise en considération des commentaires du premier cycle de certification
1.3	20/04/2017	Waterfall	Mise à jour des tableaux
1.4	12/06/2017	Waterfall	Mise à jour
1.5	09/04/2018	Waterfall	Mise à jour

Références

Code	Référence	Nom

Code	Référence	Nom
[1]	NSCIB-CC-11-34146-CR	Passerelle de sécurité unidirectionnelle Waterfall WF-400 – Rapport de certification
[2]		Profil de protection d'une diode industrielle et de ses ports (version 1.0 court terme)
[3]		Manuel d'utilisation du logiciel (version 0.1)

Page laissée volontairement libre

Sommaire

1 Introduction

1.1 Identification de la cible de sécurité

Ce document décrit la cible de sécurité relative à la plateforme WF-502F dans le but d'obtenir la Certification de Sécurité de Premier Niveau (CSPN). Cette plateforme est une diode réseau garantissant une communication unidirectionnelle entre deux réseaux informatiques à criticité différente.

1.2 Conformité du produit

Cette cible de sécurité a été rédigée selon le profil de protection suivant :

- Diode industrielle et ses ports « moyen terme » version 1.0 **Erreur ! Source du renvoi introuvable.**.

Certaines mesures de profil de protection concernent le firmware des modules RX et TX, mais ceux décrits dans le périmètre de cette cible n'en disposent pas. Certaines fonctions sont cependant assurées par le logiciel Waterfall Agent.

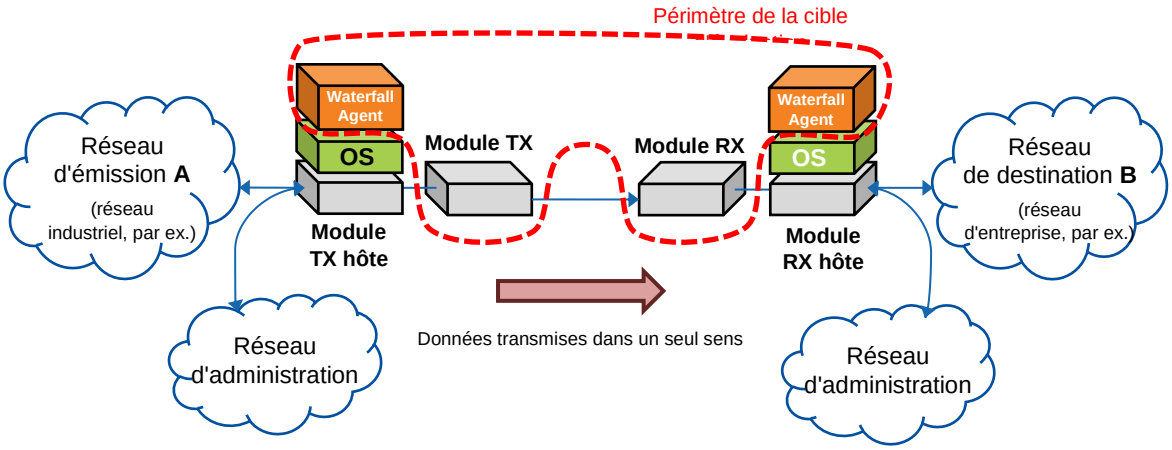
1.3 Identification du produit

Éditeur	Waterfall Security Solutions Ltd.
Lien Internet vers entreprise	www.waterfall-security.com
Dénomination commerciale du produit	WF-502F Waterfall System
Références des produits évalués	WF-502F-TX, WF-502F-RX, et le logiciel Waterfall Agent version 6.0.0.1
Catégorie de produit	Communication sécurisée

2 Informations produit

2.1 Description générale du produit

La plateforme WF-502F (cible d'évaluation) offre une solution destinée à sécuriser les échanges entre deux réseaux. Pour ce faire, la plateforme met en place un lien physique unidirectionnel par le biais d'une fibre optique. Ainsi, les données sont transmises dans un seul sens du réseau d'émission A (un réseau industriel critique, par ex.) vers le réseau de destination B (le réseau principal de la société ou un réseau de supervision, par ex.). Ce type d'équipement est également appelé diode réseau.



Le coeur de cette plateforme *passerelle* WF-502F se compose de deux dispositifs, le module TX (réf. WF-502F-TX) et le module RX (réf. WF-502F-RX). Le module TX est raccordé au réseau d'émission et le module RX est raccordé au réseau de destination. Ces deux modules sont raccordés entre eux par une fibre optique unique.

La plateforme comprend également deux « guichets» : le module TX hôte et le module RX hôte[1]. Ils se trouvent respectivement dans le réseau d'émission et le réseau de destination. Ces modules hôtes (réf. WF-502F-HOST en version complète) sont des ordinateurs de type PC sur lesquels est chargé un OS (système d'exploitation) : Windows ou Linux CentOS. Ce système d'exploitation est nécessaire au bon fonctionnement du logiciel Waterfall Agent, seul composant des modules hôtes à faire partie du périmètre de la cible d'évaluation.

Le logiciel Waterfall Agent est exécuté sur chaque guichet, composé de plusieurs services ayant chacun une tâche définie. Ils permettent de mener et de configurer toutes les tâches dont sont responsables les modules Hôtes. Le logiciel permet de configurer et de superviser les protocoles industriels Modbus et transfert de fichiers.

Remarque : Uniquement aux fins d'évaluation, Modbus Poll version 5.0.1 build 450 a été fourni avec le système de simulation. ModBus est un logiciel tiers et ne fait pas partie du logiciel Waterfall.

Le logiciel Waterfall Agent peut être livré par Waterfall Security Solutions Ltd. et déployé par un *Installer* sur un ordinateur fourni par l'utilisateur final et compatible pour héberger ce logiciel. L'utilisateur ne recevra que les modules RX et TX et le logiciel Waterfall Agent pour les modules Host.

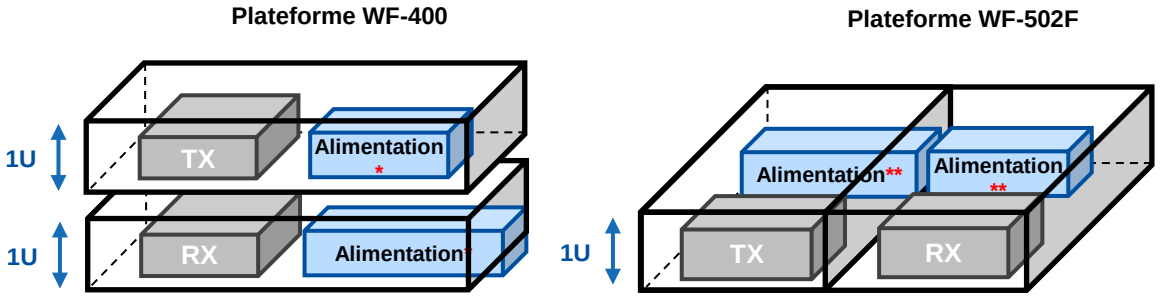
Remarque : *aucun manuel d'utilisation n'est fourni pour l'Installer Windows. Le système est*

[1] Le terme *port* se réfèrera ci-après au *module Hôte*

fourni tel quel, sous forme d'image préconfigurée.

Les cartes électroniques présentes à la fois dans le module TX (réf. 930A0701-02) et le module RX (réf. 930A0702-02) ont fait l'objet de la certification des Critères Communs (CC) au niveau EAL4 plus niveaux AVA_VAN.5, ALC_DVS.2 et ALC_FLR.2 pour une version précédente du produit (WF-400)**Erreur ! Source du renvoi introuvable.**. Le périmètre d'évaluation pour la certification CSPN est élargi au logiciel Waterfall Agent.

La principale différence entre les deux versions réside au niveau du conditionnement des modules ; la version WF-400 nécessitait deux unités TX et RX (contenant respectivement le module en question, et chacune équipée d'au moins un bloc d'alimentation). Deux emplacements (à savoir 2U) étaient ainsi nécessaires dans un rack de serveur. Désormais, avec la nouvelle plate-forme WF-502F dans sa configuration *standard*, il est possible d'utiliser un seul emplacement (à savoir 1U) pour le module TX, le module RX et les deux blocs d'alimentation de chaque module.



* : l'unité d'alimentation peut contenir un ou deux blocs d'alimentation en fonction de la configuration

Ainsi, lorsque les modules TX et RX doivent être placés à des endroits différents, il est possible de déployer une configuration *Split*.

Lorsque la disponibilité de la diode est essentielle au point d'exigence, pour un fonctionnement redondant, les configurations de *haute disponibilité* peuvent être déployées. Chacune de ces configurations comprend deux modules RX et deux modules TX.

2.2 Caractéristiques du produit

La cible d'évaluation offre les caractéristiques suivantes :

- Unidirectionnalité des flux : La cible d'évaluation garantit l'unidirectionnalité des flux du module hôte TX vers le module hôte RX.
- Terminaison protcolaire. Les modules hôtes de la cible d'évaluation fournissent la terminaison protocolaire des réseaux d'émission et de destination. La configuration de la cible d'évaluation doit être entièrement transparente pour les deux réseaux.
- Administration des services : Chaque module hôte est équipé d'une interface d'administration permettant une configuration unique des services ou des modules et la consultation et/ou l'extraction des journaux d'événements enregistrés.

  Un mécanisme d'authentification exige des administrateurs de s'identifier pour effectuer les opérations avec les outils de configuration et de surveillance Waterfall. La cible d'évaluation stocke les identifiants et applique une politique de mot de passe. Pour de plus amples précisions, consulter le manuel d'utilisation**Erreur ! Source du renvoi introuvable.**.

- Journalisation : Les modules hôtes permettent par l'intermédiaire du logiciel Waterfall Agent de définir une politique pour la journalisation locale et distante des événements gérés par les divers services du logiciel Waterfall Agent.

2.3 Utilisation du produit

La cible d'évaluation est généralement utilisée pour fournir l'interface entre deux réseaux aux degrés de sensibilité différents. Le cas examiné est celui des échanges entre ces deux réseaux lorsqu'ils sont bâtis de plus critique à moins critique. Après le raccordement du module TX au réseau d'émission, du module RX au réseau de destination et des deux modules à la fibre optique, le flux de données est le suivant :

1) Les données transmises par le réseau d'émission sont reçues et traitées par le module TX par l'intermédiaire du logiciel Waterfall Agent.
2) Les données sont transmises au module TX par le câble Ethernet.
3) Le module TX transforme le signal électrique en signal optique qu'il transmet alors au module RX par la fibre optique.
4) Le module RX reçoit les données optiques et les transforme en signal électrique.
5) Le module RX transmet les données au module RX hôte par le câble Ethernet.
6) Le logiciel Waterfall Agent du module hôte reçoit les données qu'il peut alors transmettre au réseau de destination.

2.4 Environnement technique du produit

Le logiciel Waterfall Agent fonctionne en environnement Windows et Linux CentOS, architecture 32 et 64 bits.

La version du système d’exploitation utilisé dans le cadre de l’évaluation est :

- Windows 8.1 64 bits pour les hôtes TX et RX.

Le système permet une administration a distance ; cette fonctionnalité n’a pas fait l‘objet de l’évaluation , seule l’administration locale fait partie du périmètre d’évaluation.

En conséquence les modules Apache et PHP utilisés par l’administration à distance ne doivent pas être installés par l’utilisateur final en configuration CSPN..

De même l accès à distance via protocole rdp doit être desactivé

2.5 Utilisateurs du produit

La liste des utilisateurs définis dans le profil de protection **Erreur ! Source du renvoi introuvable.** est gérée par le système d'exploitation et ne fait donc pas partie du périmètre de la cible d'évaluation. L'utilisateur final est responsable de la gestion de l'accès au système et des autorisations.

Utilisateurs susceptibles d'interagir avec la cible d'évaluation :

- **Administrateur** : utilisateur ayant tous les droits sur les guichets. Il peut ainsi modifier la configuration de service de la cible d'évaluation et consulter tout ou partie des journaux d'événements produits par la cible d'évaluation. Toutefois, il ne peut en aucun cas interférer avec la fonction de sécurité de la cible d'évaluation, qui est de garantir l'unidirectionnalité des flux.
- **Utilisateur** : Utilisateur sans droits sur les guichets. Il ne peut pas modifier la configuration de service de la cible d'évaluation, ni consulter tout ou partie des journaux d'événements produits par la cible d'évaluation. De même il ne peut en aucun cas interférer avec la fonction de sécurité de la cible d'évaluation, qui est de garantir l'unidirectionnalité des flux.

2.6 Scénarios d'environnement

E. Consultation des journaux

Il est considéré que l'administrateur consulte régulièrement les journaux locaux ou distants qui sont générés par l'équipement.

E. Administrateurs

Les administrateurs sont des personnes compétentes formées à l'utilisation de la cible d'évaluation. De plus, ils sont considérés comme des gens de confiance sans l'intention de causer des dommages.

E. Environnement physique

Les modules de la cible d'évaluation ne sont pas tous nécessairement installés dans un endroit sûr et un attaquant peut avoir accès à tous les ports de la cible d'évaluation. Une fois que l'attaquant a gagné un accès physique à la cible d'évaluation, il peut connecter un dispositif piégé à un port physique de la cible d'évaluation. D'autre part, il ne peut pas démonter ou effectuer une attaque physique sur la cible d'évaluation.

E. Sens de la diode

Il est supposé que la cible d'évaluation est adaptée en fonction du type d'utilisation. La diode est notamment orientée dans le bon sens et les guichets disposent des protocoles appropriés.

E. Dimensionnement

Il est supposé que la cible d'évaluation est dimensionnée correctement pour les traitements qu'elle doit éffectuer.

E. Services non évalués et désactivés par défaut

La configuration web est désactivée par défaut dans l'équipement évalué. L'accès à distance via rdp est désactivé

E. Branchements réseau

La cible d'évaluation assure que les informations sont acheminées uniquement du réseau connecté au module TX vers le réseau connecté au module RXLa cible d’évaluation sera la seule connexion entre les 2 segments de réseau.

E. Documentation de sécurité

La cible d'évaluation est fournie avec une documentation **Erreur ! Source du renvoi introuvable.** détaillée sur l'utilisation sécurisée de l'équipement, ainsi que sur la configuration de ses différents services. Toutes les recommandations émises dans cette documentation ont été appliquées à des fins d'évaluation.

2.7 Définition du périmètre d'évaluation

La plateforme WF-502F peut accueillir différents modules, mais ici seuls le module TX, le module RX et le logiciel Waterfall Agent version 6.0.0.1 font partie du périmètre de la cible d'évaluation.

Les autres configurations de la plateforme qui n'ont pas d'incidence pas les fonctions de sécurité, telles que *Standard-Split* et *Standard Split High-Availability*, font partie du périmètre de la cible d'évaluation.

La cible d'évaluation prend en charge une multitude de protocoles et encapsule ces protocoles en protocole propriétaire. L'analyse de sécurité de ce protocole propriétaire fait partie du périmètre de la cible d'évaluation. Par exemple, la configuration de test utilisée pour l'évaluation prend en charge les protocoles Modbus et transfert de fichiers.

La fibre optique raccordant le module TX au module RX ne fait pas partie du périmètre de la cible d'évaluation.

Les machines et le système d'exploitation des modules hôtes qui hébergent le logiciel Waterfall Agent ne font pas partie du périmètre de la cible d'évaluation.

Pour cette évaluation, la configuration à distance (interface web) est désactivée, seule la configuration de l’équipement est évaluée. Seule la configuration locale de l’équipement est évaluée.

3 Biens sensibles que le produit doit protéger

3.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivantes :

S. Réseau critique

La cible d'évaluation protège le réseau le plus critique en garantissant l'unidirectionnalité des échanges uniquement vers le réseau de destination.

S. Échanges par la diode

La cible de l'évaluation assure la transmission des données entre le module TX et le module RX.

Les besoins de sécurité des biens sensibles de l'environnement sont les suivantes :

Biens	Disponibilité	Confidentialité	Intégrité	Authenticité
B. Réseau critique	X		X	
S. Échanges par la diode	X		X	

3.2 Biens sensibles de la cible d'évaluation

Les biens sensibles de la cible d'évaluation sont :

S. Firmware des guichets

Les modules TX et RX n'ont pas de firmware. Leur puce FPGA et le microcode associé ne font pas partie du périmètre de la cible d'évaluation.

S. Configuration des guichets

Les guichets ne disposent pas de fonctions de sécurité configurables. Il n'existe ainsi aucune obligation d'assurer la confidentialité et l'intégrité de cette configuration.

S. Politique de gestion des droits

Aucune politique des droits n'a été mise en place dans la cible d'évaluation. La gestion des droits n'est pas du domaine du logiciel Waterfall Agent. Toutefois, il convient de noter que la politique de gestion des droits peut être mise en place dans l'environnement de la cible d'évaluation par l'intermédiaire du système d'exploitation.

S. Fonction de journalisation locale

La cible d'évaluation, par l'intermédiaire de Waterfall Agent, a une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle. Cette fonction est assurée par un service Waterfall Agent et son but est de consigner les événements de divers autres services.

S. Fonction de journalisation distante

La cible d'évaluation, par l'intermédiaire de Waterfall Agent, a une fonction de journalisation distante qui, une fois configurée, doit rester opérationnelle. Cette fonction est assurée par un service Waterfall Agent et son but est de consigner les événements de divers autres services. Elle consiste à transmettre les journaux générés par la fonction locale.

S. Journaux des évènements locaux

Les journaux des évènements locaux générés par la cible d'évaluation doivent être intègres.

S. Journaux des évènements distants

L'intégrité des journaux distants émis par la cible d'évaluation doit être assurée. Le mécanisme doit également permettre au destinataire de détecter l'absence d'un message dans une suite de messages reçus correctement.

Les exigences de sécurité des biens sensibles de la cible d'évaluation sont les suivantes :

Biens	Disponibilité	Confidentialité	Intégrité	Authenticité
B. Fonction de journalisation locale	X			
B. Fonction de journalisation distante	X			
B. Journaux des évènements locaux			X	X
B. Journaux des évènements distants			X	

4 Menaces

4.1 Agents menaçants

Les agents menaçants suivants ont été retenus :

- Un ordinateur ou une application connecté à la cible d'évaluation et contrôlé par un attaquant
- Une personne interne ou externe, ayant ou non l'intention de causer des dommages et ayant accès au réseau d'émission et/ou au réseau de destination

Par hypothèse, les administrateurs ne sont pas à considérer comme attaquants potentiels.

4.2 Menaces retenues

Pour le périmètre de la cible d'évaluation, ont été utilisées les menaces suivantes :

T. Déni de service

Un attaquant parvient à effectuer un déni de service sur la cible d'évaluation en provoquant un événement non géré ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu, etc.). Ce déni de service peut affecter l'ensemble de la cible d'évaluation ou seulement certaines de ses fonctions.

T. Violation de l'unidirectionnalité des échanges

Un attaquant ayant accès au réseau de destination parvient à transférer des informations du réseau de destination (guichet RX) au réseau d'émission (guichet TX).

T. Contournement d'authentification

La gestion de l'authentification au système d'exploitation est hors du périmètre de la cible d'évaluation. Une exception est faite pour l'authentification aux produits SW de configuration et de surveillance Waterfall localement.

T. Corruption des journaux d'événements locaux

L'attaquant parvient à supprimer ou modifier une entrée dans le journal des événements locaux sans en avoir été autorisé par la politique des droits de la cible d'évaluation.

T. Corruption des journaux d'événements distants

L'attaquant parvient à modifier une entrée dans le journal distant émis par la cible d'évaluation à l'insu du destinataire. L'attaquant parvient à supprimer un journal distant émis, à l'insu du destinataire.

5 Fonctions de sécurité du produit

F. Gestion des entrées malformées

La cible d'évaluation a été développée afin de gérer correctement les entrées malformées, en particulier celles provenant du réseau d'émission.

F. Unidirectionnalité des flux d'informations

L'unidirectionnalité des flux est physiquement garantie par la cible d'évaluation. Ce contrôle du sens du flux d'informations est garanti par l'utilisation d'émetteurs-récepteurs SFP (ou *Small Form-factor Pluggable*) spécifiques :

- Pour le module TX, le SFP ne dispose que d'un émetteur optique. La partie réception est physiquement absente du SFP.
- Pour le module RX, le SFP ne dispose que d'un récepteur optique. La partie émission est physiquement absente du SFP.

F. Authentification sécurisée

Les noms d'utilisateur et les mots de passe sont stockés dans une base de données et servent tous les produits Waterfall : outil de configuration.

F. Stockage sécurisé des mots de passe

Les informations d'identification de la cible d'évaluation sont hachées. Waterfall applique une politique de mot de passe, comme décrit dans le manuel d'utilisation**Erreur ! Source du renvoi introuvable.**.

F. Intégrité des journaux

Les journaux d'événements générés par la cible d'évaluation sont intégrés et seul l'administrateur du système d'exploitation est en mesure de les modifier.

A. Ressources par menaces

	Réseau critique	Échanges par la diode	Firmware de port	Configuration des ports	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux des évènements locaux	Journaux des évènements distants
Déni de service	X	X				X			
Violation de l'unidirectionnalité des échanges	X	X							
Contournement d'authentification						X	X		
Contournement de la politique des droits					X				
Corruption des journaux d'évènements locaux	X	X							
Corruption des journaux d'évènements distants							X		X

B. Menaces par fonctions de sécurité

	Déni de service	Violation de l'unidirectionnalité des échanges	Contournement d'authentification	Contournement de la politique des droits	Corruption des journaux d'évènements locaux	Corruption des journaux d'évènements distants
F. Gestion des entrées malformées	x					
F. Unidirectionnalité des flux d'informations		x				
F. Authentification sécurisée			x			
F. Intégrité des journaux					x	
F. Stockage sécurisé des mots de passe			x			