Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2016/09

Siemens

Scalance XM408-8C

Version du micrologiciel 05.01.00

Paris, le 13 juin 2016

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2016/09

Nom du produit

SCALANCE XM408-8C

Référence/version du produit

Version du micro-logiciel 05.01.00

Référence de la cible de sécurité

Cible de sécurité

Référence : CSPN-ST-SCALANCE_XM400-2.02 en date du 18 mai 2016.

Catégorie de produit

Commutateur industriel

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Siemens S.A.S

40, Avenue des Fruitiers
93527 Saint-Denis
France

Centre d'évaluation

Amossys

4 bis allée du bâtiment, 35000 Rennes, France

Fonctions de sécurité évaluées

Gestion des entrées malformées
Politique de cloisonnement logique
Connexion sécurisée avec le serveur d'authentification
Authentification sécurisée sur l'interface d'administration
Politique de droits
Signature du firmware
Intégrité et confidentialité de la configuration

Fonctions de sécurité non évaluées

Stockage sécurisé des secrets

Restrictions d'usage

Oui (cf. §3.2)

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le commutateur industriel Scalance XM408-8C, version 05.01.00 développé par *SIEMENS*.

Un commutateur industriel doit pouvoir fonctionner dans des conditions ambiantes hostiles. En particulier, il doit pouvoir fonctionner en présence d'humidité ou de poussière, ou avec des températures inhabituelles pour des équipements informatiques.
Ce commutateur industriel permet d'interconnecter différents équipements ou segments de réseaux communiquant en Ethernet. Il supporte la fonctionnalité VLAN (Virtual Local Area Network) et permet ainsi d'effectuer du cloisonnement réseau logique.
Les commutateurs industriels peuvent être utilisés pour assurer un cloisonnement logique entre les réseaux de terrains qui relient les entrées-sorties déportées des automates programmables industriels et les réseaux de supervisions qui relient ces automates aux stations SCADA. En outre ce cloisonnement peut être employé pour les fonctions d'administration des stations SCADA ou de ces mêmes commutateurs.
Ainsi dans l'exemple de la Figure 1, le commutateur permet à chaque automate de ne communiquer qu'avec un capteur et un actionneur (VLAN 2 et 3) et empêche la communication entre les deux automates (VLAN 2 et 3 sur le réseau du bas et 4 et 5 sur celui du haut). Enfin, les fonctions d'administration des commutateurs et du poste SCADA sont isolées des autres réseaux (VLAN 1).

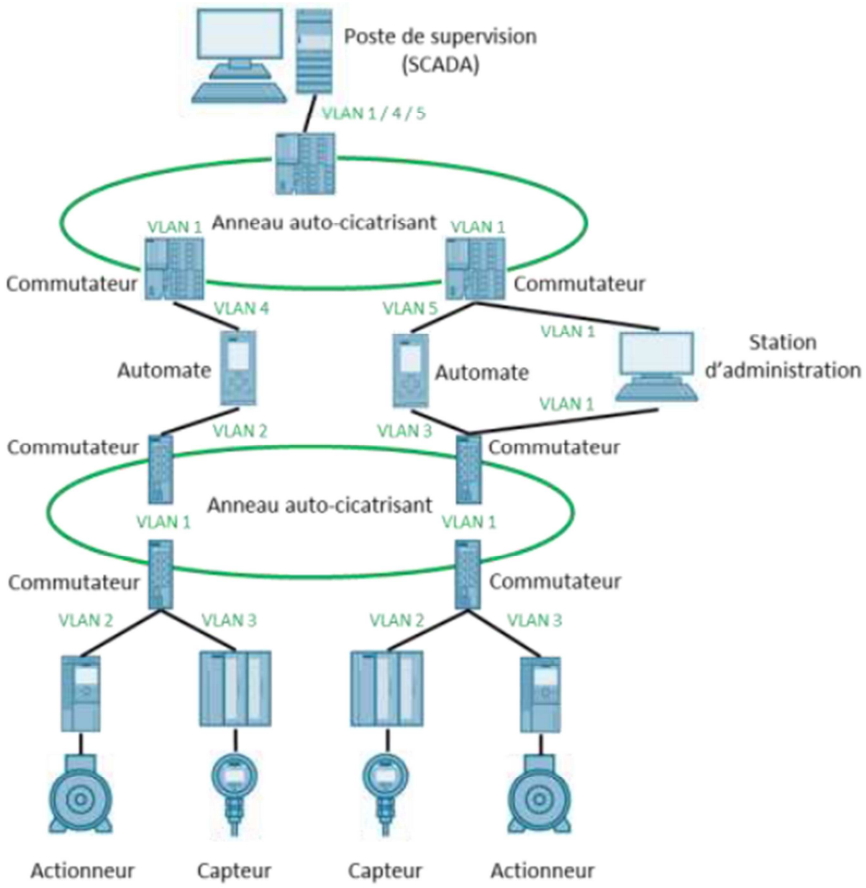

Figure 1 – Réseaux avec cloisonnement par VLAN.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☐ 6 – identification, authentification et contrôle d'accès
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 – environnement d'exécution sécurisé
☐ 11 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☐ 13 – automate programmable industriel
☒ **14 – autre : commutateur industriel**

1.2.2. Identification du produit

Nom du produit	Scalance XM408-8C
Numéro de la version analysée	05.01.00

La version certifiée du produit peut être identifiée au travers de l'interface d'administration via les menus [Information > Versions].

1.2.3. Configuration évaluée

Le commutateur est livré sous la forme d'un boîtier, la configuration évaluée est celle par défaut.
La fonction *Near Field Communications* (NFC) n'est pas activée dans la configuration par défaut et ne doit pas l'être.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

La plateforme de test est constituée des éléments suivants :

- un commutateur XM408-8C ;
- une station d'administration Linux Debian 8 64 bits ;
- un automate programmable industriel Simatic S7 1518-4 ;
- un serveur Radius Windows Server 2012 R2 ;
- deux stations Linux Debian 8 64 bits respectivement dans les VLAN 1 et 2 ;
- une machine connectée au réseau d'administration ou sur les VLAN dans le rôle de l'attaquant, fonctionnant selon les tests sur les systèmes d'exploitation suivants : Debian 8 64 bits, Kali 64 bits ou Windows 8 64 bits.

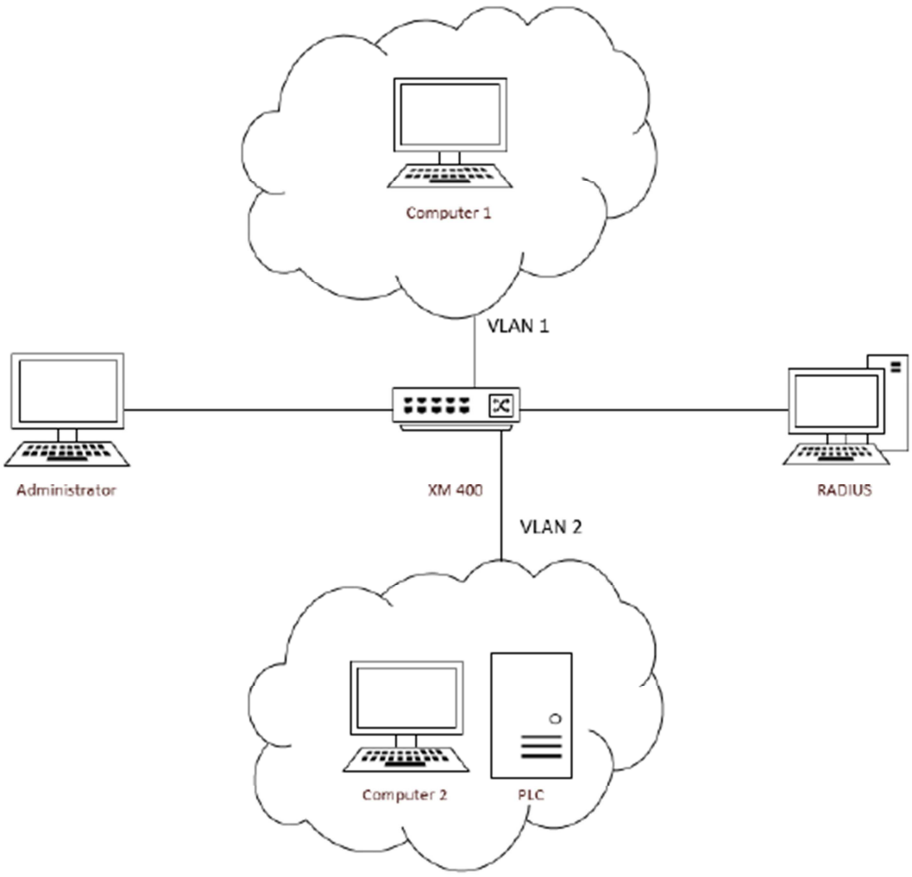

Figure 2 – Plateforme de test.

2.3.1.2. Particularités de paramétrage de l'environnement et options d'installation

Le commutateur a été évalué dans la configuration précisée au paragraphe 1.2.3.

2.3.1.3. Description de l'installation et des non-conformités éventuelles

Néant.

2.3.1.4. Durée de l'installation

L'installation de la plateforme de test a nécessité deux jours.

2.3.1.5. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

La documentation est claire et correctement rédigée.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

2.3.4. Analyse de la conformité des fonctions de sécurité

Le « stockage sécurisé des secrets » compte tenu du type d'évaluation en boite noire n'a pas pu faire l'objet de tests.
La fonction de sécurité « signature du *firmware* » a bien fait l'objet de tests qui ont montré qu'un *firmware* malformé est rejeté par la cible, qui n'a pas ainsi été mise en défaut. Cependant compte tenu de l'évaluation en boite noire, il n'est pas possible de démontrer la présence d'un mécanisme de protection de l'intégrité du *firmware*.

Les autres fonctions de sécurité ont été testées et sont conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité testées ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation de la cible d'évaluation.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues et exploitables sur ce produit dans sa version évaluée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit ou à son implémentation pouvant remettre en cause la sécurité du produit sur le périmètre évalué et ses fonctions de sécurité. En revanche l'interface d'administration web est vulnérable à des attaques pouvant conduire à un déni de service de celle-ci (le commutateur reste dans ce cas fonctionnel). Aussi des recommandations sont émises au paragraphe 2.3.8.2 afin de se prémunir contre de telles attaques.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur du produit devra mettre en œuvre les mesures suivantes :

- l'interface d'administration *Web Based Management*, doit être cloisonnée sur un seul VLAN (par défaut le VLAN 1) ;
- l'accès à l'interface d'administration *Web Based Management* doit être uniquement réalisée en HTTPS et par conséquent http doit être désactivé ;
- l'accès à l'interface d'administration doit être restreint aux seules stations d'administration grâce au filtre *Access Control List* (ACL) ;

- sur les ports transportant plusieurs VLAN, l'ensemble des trames doivent être *taggées* 802.1Q ;
- sur les ports transportant plusieurs VLAN, seules les trames *taggées* 802.1Q doivent être acceptées, ainsi l'option *Acceptable Frames* doit être positionnée à *Tagged Frames Only* ;
- les ports transportant un unique VLAN doivent activer l'option *Ingress Filtering*.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Sans objet.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit Scalance XM408-8C, version 05.01.00 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur de ce certificat devra s'attacher à employer la configuration énoncée au paragraphe 1.2.3 et suivre les recommandations décrites au paragraphe 2.3.8.2.

Enfin les règles de défense en profondeurs doivent être appliquées, les administrateurs doivent aussi mettre en place une politique de gestion et de dimensionnement de mots de passe conformes aux recommandations de l'ANSSI.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN Scalance XM408-8C* Référence : CSPN-ST-SCALANCE_XM408-8C-2.02 ; Version : 2.02 ; Date : *18 mai 2016.*
[RTE]	*CSPN Evaluation Technical Report Product SCALANCE-XM408-8C version 05.01.00* Référence : CSPN-ETR-SCALANCE-1.03 ; Version : 1.03 ; Date : *19 mai 2016.* *Technical Note* Référence : NT-DR-SCALANCE-1.01 Version : 1.01 ; Date : 2 mai .2016.
[GUIDES]	*SIMATIC NET Industrial Ethernet switches SCALANCE XM-400/XR-500 Web Based Management* Référence : *C79000-G8976-C248-09* ; Date : *mars 2015*.

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur http://www.ssi.gouv.fr/
[NOTE-3]	Méthodologie pour l'évaluation logicielle d'automates programmables industriels en vue d'une certification de sécurité de premier niveau ANSSI-CSPN-NOTE-03/1 du 30 juillet 2015. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 2.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03. Documents disponibles sur http://www.ssi.gouv.fr/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.