



IT Security Alert Alerte de sécurité TI

7 December 2007

ITSA-46

Le 7 décembre 2007

Secure Fax Transmission Using Secure Communications Interoperability Protocol Devices

Transmission de télécopies sécurisées à l'aide de dispositifs compatibles au protocole d'interopérabilité des communications sécurisées

Purpose

The purpose of this Alert is to provide Secure Communications Interoperability Protocol (SCIP) users with secure fax guidance.

Instructions for sending secure faxes with the Secure Telephone Equipment (STE), OMNI, and the Secure Wireline Terminal (SWT) can be found in Annex A, Annex B, and Annex C of this Alert.

CSEC does not have definite solutions for all secure fax problems; however, CSEC is working diligently to address these issues.

Background

Secure fax configuration problems may be encountered as users adjust to the SCIP devices.

Users have noted intermittent compatibility problems when using SCIP devices with secure faxes because of the variety of combinations and permutations of secure fax models and communications links.

Users should note that increased usage may reveal equipment compatibility issues that have not yet been

Objet

La présente alerte vise à informer les utilisateurs de produits compatibles au protocole d'interopérabilité des communications sécurisées (SCIP pour *Secure Communications Interoperability Protocol*) sur des directives relatives à la transmission de télécopies sécurisées.

Des instructions sur la transmission de télécopies sécurisées à l'aide du Secure Telephone Equipment (STE), de l'OMNI et du Secure Wireline Terminal (SWT) sont données à l'Annexe A, l'Annexe B et l'Annexe C, respectivement, de la présente alerte.

Le CSTC n'a pas de solutions définitives pour remédier à tous les problèmes liés à la télécopie sécurisée, mais il y travaille avec diligence.

Contexte

Il est possible que les utilisateurs SCIP rencontrent des problèmes liés à la configuration des télécopieurs sécurisés au fur et à mesure qu'ils s'habituent à utiliser leur dispositif SCIP.

Certains utilisateurs ont signalé des problèmes intermittents de compatibilité durant l'utilisation d'un dispositif SCIP avec des télécopieurs sécurisés en raison de la grande variété de combinaisons et de

identified.

permutations possibles des modèles de télécopieur sécurisé et de liaisons de données.

Il est à noter qu'une utilisation accrue pourrait révéler d'autres problèmes de compatibilité qui n'ont pas encore été cernés.

Secure Faxing with STE

There are three known technical issues that could be encountered when using STE devices for secure fax transmissions: Secure Call Failed message on the STE; transmission error on the secure fax; and the complete lock-up of either the secure fax or STE.

In order to minimize potential error situations, users should ensure that the STE and the secure fax have been properly configured by following the instructions found in Annex A of this Alert.

CSEC provides the following guidance to users who experience STE error messages:

Secure Call Failed Message on STE – Hang up receiver, re-establish secure data call, and begin re-transmitting from the failed page onward.

Transmission error on secure fax – If the secure line is still active, it is possible to re-send the document without ending the secure call. Start re-sending the document from the failed page onward.

Lock-up of STE or secure fax – Reset the STE and the secure fax by making sure that both devices are powered off at the same time. Then turn on the secure fax followed by the STE.

General Recommendations

CSEC provides the following recommendations to assist secure fax and SCIP users:

- 1) In order to allow for maximum interoperability between users, the recommended configuration for secure faxing with SCIP devices is: MODE

Télécopie sécurisée à l'aide du STE

Trois erreurs techniques connues peuvent survenir lorsqu'on utilise un STE pour transmettre des télécopies sécurisées, soit l'affichage d'un message d'échec de communication sécurisée sur le STE, une erreur de transmission sur le télécopieur sécurisé et le verrouillage complet du télécopieur sécurisé ou du STE.

Afin d'éviter toute possibilité d'erreur, les utilisateurs devraient s'assurer que le STE et le télécopieur sécurisé ont été configurés correctement en suivant les instructions données à l'Annexe A de la présente alerte.

Le CSTC recommande la marche à suivre ci-après en présence d'une condition d'erreur sur le STE :

Message du STE : *Secure Call Failed* – Raccrocher le combiné, rétablir la communication de données sécurisée et recommencer la transmission à partir de la page échouée.

Erreur de transmission sur le télécopieur sécurisé – Si la ligne sécurisée est toujours active, il est possible d'envoyer de nouveau le document sans mettre fin à l'appel sécurisé. Recommencer la transmission à partir de la page échouée.

Verrouillage du STE ou du télécopieur sécurisé – Réinitialiser le STE et le télécopieur sécurisé en veillant à éteindre les deux appareils en même temps. Rallumer ensuite le télécopieur, puis le STE.

Recommandations générales

Le CSTC recommande ce qui suit aux utilisateurs SCIP qui veulent effectuer des télécopies sécurisées :

- 1) Afin de permettre une interopérabilité maximale entre les utilisateurs, la configuration recommandée pour la télécopie sécurisée à l'aide

- 03 (ASYNC 9.6).
- 2) Users operating older secure fax models that only support the synchronous data modes should replace their secure faxes with newer models that can operate in asynchronous data modes. The asynchronous capability should be confirmed with the vendor before committing to any purchase.
 - 3) CSEC recommends that STE users remain at release 2.4, if possible. Unfortunately, it is not possible to revert back to release 2.4 once the upgrade to release 2.5 has been completed.
 - 4) In order to ensure GC secure fax interoperability as a whole, users should coordinate secure fax and SCIP equipment configuration status with Canadian contacts and international partners.
- de dispositifs SCIP est : MODE 03 (ASYNC 9.6).
- 2) Les utilisateurs d'anciens modèles de télécopieur qui ne prennent en charge que les modes données synchrones devraient remplacer leurs appareils par des modèles plus récents qui peuvent fonctionner dans des modes données asynchrones. Il faudrait confirmer la capacité de transmission asynchrone auprès du fournisseur avant de s'engager à acquérir un appareil.
 - 3) Les utilisateurs devraient demeurer à la version logicielle 2.4, dans la mesure du possible. Malheureusement, il n'est pas possible de retourner à la version 2.4 après avoir effectué une mise à niveau à la version 2.5
 - 4) Afin d'assurer l'interopérabilité sécurisée du GC dans son ensemble, les utilisateurs devraient coordonner la configuration des télécopieurs sécurisés et des dispositifs SCIP avec les contacts canadiens et les partenaires internationaux.

Contacts and Assistance

For further information or guidance, contact the Crypto Material Assistance Centre (CMAC) at (613) 991-8600.

e-mail: cmac@cse-cst.gc.ca

For technical assistance, contact CSEC Technical Support at (613) 991-7496

e-mail: securephones@cse-cst.gc.ca

Aide et renseignements

Pour plus de renseignements ou d'assistance, prière de communiquer avec le Centre d'assistance en matière de matériel cryptographique (CAMC) au 613-991-8600.

Courriel : cmac@cse-cst.gc.ca

Pour une assistance technique, prière de communiquer avec le Soutien technique du CSTC au 613-991-7496.

Courriel : securephones@cse-cst.gc.ca

La directrice de la Gestion de la mission de la Sécurité des TI,



Gwen Beauchemin
Director, IT Security Mission Management