

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de WinSCP

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-408>

Gestion du document

Référence	CERTA-2007-AVI-408
Titre	Vulnérabilité de WinSCP
Date de la première version	19 septembre 2007
Date de la dernière version	–
Source(s)	Changement de version WinSCP du 02 septembre 2007
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- atteinte à la confidentialité, l'intégrité et la disponibilité des données ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- La version 4.0.3 de WinSCP ainsi que celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans l'outil de transfert de données WinSCP. L'exploitation de cette dernière permettrait à une personne distante d'effectuer de forcer des transactions illégitimes à un utilisateur ayant une version de WinSCP vulnérable.

4 Description

Une vulnérabilité a été identifiée dans l'outil de transfert de données WinSCP. L'installation de l'application spécifique au système d'exploitation les protocoles qu'il peut manipuler : `scp://` et `sftp://`. Une personne

malveillante qui contrôlerait un serveur FTP peut forcer sa victime à effectuer des transferts de données par une adresse construite à partir de ces protocoles. Il peut s'agir d'un lien ajouté dans le champ IFRAME d'une page par exemple. Le transfert peut être dans les deux sens : chargement ou récupération de données sur le poste ayant une version de WinSCP vulnérable.

5 Solution

Se référer au bulletin de sécurité et installer la version 4.0.4 de WinSCP disponible sur le site du projet (cf. section Documentation).

6 Documentation

- Version 4.0.4 disponible sur le site du projet WinSCP :
<http://winscp.net/eng/download.php>
- Documentation en français de WinSCP :
<http://winscp.net/eng/docs/lang:fr>
- Référence CVE CVE-2007-4909 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4909>

Gestion détaillée du document

19 septembre 2007 version initiale.