

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco IronPort

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-2009-AVI-016>

Gestion du document

Référence	CERTA-2009-AVI-016-001
Titre	Multiples vulnérabilités dans Cisco IronPort
Date de la première version	15 janvier 2009
Date de la dernière version	16 janvier 2009
Source(s)	Bulletin de sécurité Cisco #109329 du 14 janvier 2009
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 des données ;
- injection de code indirecte (*Cross-site Scripting*).

2 Systèmes affectés

- Toutes les versions de Cisco PostX 6.2.1 antérieures à la 6.2.1.1 ;
- toutes les versions de Cisco PostX 6.2.2 antérieures à la 6.2.2.3 ;
- toutes les versions de Cisco IronPort Encrytion Appliance/PostX 6.2.4 antérieures à la 6.2.4.1.1 ;
- toutes les versions de Cisco IronPort Encrytion Appliance/PostX 6.2.5 ;
- toutes les versions de Cisco IronPort Encrytion Appliance/PostX 6.2.6 ;
- toutes les versions de Cisco IronPort Encrytion Appliance/PostX 6.2.7 antérieures à la 6.2.7.7 ;
- toutes les versions de Cisco IronPort Encrytion Appliance/ 6.3 antérieures à la 6.3.0.4 ;
- toutes les versions de Cisco IronPort Encrytion Appliance 6.5 antérieures à la 6.5.0.1.

3 Résumé

Plusieurs vulnérabilités présentes dans Cisco IronPort permettent à un utilisateur distant de porter atteinte à la confidentialité de certaines données ou de réaliser des attaques de type injection de code indirecte.

4 Description

Plusieurs vulnérabilités sont présentes dans Cisco IronPort :

- la première permet à un utilisateur distant d’obtenir la clef de déchiffrement d’un message ne lui étant pas destiné et ainsi de consulter son contenu ;
- la deuxième, de nature non précisée par l’éditeur, permet également à un utilisateur distant malintentionné d’obtenir les identifiants d’un autre utilisateur ainsi que le contenu « en clair » de ses messages chiffrés.
- la dernière vulnérabilité est relative à l’interface d’administration du produit qui présente une faille de type injection de code indirecte. Elle permet à un utilisateur distant malintentionné de modifier à l’insu d’un utilisateur cible les données de son profil, y compris ses identifiants de connexion, par le biais d’une page *web* construite de façon particulière.

5 Solution

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco #109329 du 14 janvier 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090114-ironport.shtml>
- Référence CVE CVE-2009-0053 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0053>
- Référence CVE CVE-2009-0054 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0054>
- Référence CVE CVE-2009-0055 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0055>
- Référence CVE CVE-2009-0056 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0056>

Gestion détaillée du document

15 janvier 2009 version initiale ;

16 janvier 2009 correction des versions affectées pour les versions 6.3 et 6.5.