

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits ISS

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-2006-AVI-314>

Gestion du document

Référence	CERTA-2006-AVI-314
Titre	Vulnérabilité dans les produits ISS
Date de la première version	27 juillet 2006
Date de la dernière version	–
Source(s)	Alerte de sécurité de ISS (Internet Security Systems) du 26 juillet 2006
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

Déni de service à distance.

2 Systèmes affectés

- ISS BlackICE PC Protection 3.6 ;
- ISS BlackICE Server Protection 3.6 ;
- ISS Proventia A Series ;
- ISS Proventia G Series ;
- ISS Proventia M Series ;
- ISS Proventia Desktop ;
- ISS Proventia Server ;
- ISS RealSecure Desktop ;
- ISS RealSecure Network Sensor 7.0 ;
- ISS RealSecure Server Sensor 7.0.

3 Résumé

Une vulnérabilité a été identifiée dans les produits ISS RealSecure/BlackICE. Une personne malveillante peut envoyer un paquet spécialement conçu utilisant cette dernière afin de créer un déni de service sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans les outils de sécurité d'ISS RealSecure/BlackICE. Ils analysent le protocole SMB/TCP afin de détecter des codes malveillants visant la vulnérabilité SMB Mailhost décrite dans l'avis Microsoft MS06-035. Cependant, la phase d'analyse n'est pas correctement effectuée, et du trafic pouvant être légitime cause une erreur dans le système affecté, ou provoque une perte de connexion nécessitant un redémarrage. Une personne malveillante peut également envoyer des paquets similaires afin de créer un déni de service.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs, prénommés XPU (XPU 24.40) par ISS (cf. section Documentation).

6 Documentation

- Référence CVE CVE-2006-3840 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3840>
- Alerte de sécurité de ISS (Internet Security Systems) du 26 juillet 2006 :
<http://xforce.iss.net/xforce/alerts/id/230>
- Site de mise à jour d'ISS :
<http://www.iss.net/download>
- Bulletin de sécurité Microsoft MS06-035 du 11 juillet 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-035.msp>
- Avis du CERTA CERTA-2006-AVI-283 correspondant au bulletin Microsoft MS06-035 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-283/>

Gestion détaillée du document

27 juillet 2006 version initiale.