



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 22 mars 2004
N° CERTA-2004-AVI-096-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des produits Proventia, BlackICE et RealSecure d'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-2004-AVI-096>

Gestion du document

Référence	CERTA-2004-AVI-096-001
Titre	Vulnérabilité des produits Proventia, BlackICE et RealSecure d'ISS
Date de la première version	19 mars 2004
Date de la dernière version	22 mars 2004
Source(s)	Avis AD20040318 d'Eeye
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- RealSecure Network 7.0, XPU 22.11 et versions antérieures ;
- RealSecure Server Sensor 7.0 XPU 22.11 et versions antérieures ;
- RealSecure Server Sensor 6.5 for Windows SR 3.10 et versions antérieures ;
- Proventia A Series XPU 22.11 et versions antérieures ;
- Proventia G Series XPU 22.11 et versions antérieures ;
- Proventia M Series XPU 1.9 et versions antérieures ;
- RealSecure Desktop 7.0 ebl et versions antérieures ;
- RealSecure Desktop 3.6 ecf et versions antérieures ;
- RealSecure Guard 3.6 ecf et versions antérieures ;
- RealSecure Sentry 3.6 ecf et versions antérieures ;
- BlackICE Agent for Server 3.6 ecf et versions antérieures ;
- BlackICE PC Protection 3.6 ccf et versions antérieures ;
- BlackICE Server Protection 3.6 ccf et versions antérieures.

3 Résumé

Une vulnérabilité dans le composant PAM (Protocol Analysis Module) lors du traitement des réponses des serveurs ICQ permet l'exécution de code arbitraire à distance.

4 Description

Le composant PAM (Protocol Analysis Module) facilite la reconnaissance des protocoles réseau. Les paquets ayant comme port source le port 4000/udp seront considérés comme étant des réponses d'un serveur ICQ v5. Une vulnérabilité dans la routine de traitement du protocole ICQ du composant PAM dans les produits ISS cités (voir Systèmes affectés) permet à un utilisateur mal intentionné d'exécuter de code arbitraire à distance avec les droits SYSTEM sur les agents RealSecure/BlackICE.

5 Contournement provisoire

Filtrer le port *source* 4000/UDP au niveau du pare-feu.

6 Solution

Appliquer le correctif d'ISS :
<http://www.iss.net/download>

7 Documentation

- Avis AD20040318 d'Eeye :
<http://www.eeye.com/html/Research/Advisories/AD20040318.html>
- Alerte id 166 d'ISS :
<http://xforce.iss.net/xforce/alerts/id/166>
- Avis CERTA-2004-AVI-053 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-053/>

Gestion détaillée du document

19 mars 2004 version initiale.

22 mars 2004 précisions sur le contournement provisoire.