

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-053>

Gestion du document

Référence	CERTA-2004-AVI-053
Titre	Vulnérabilité des produits Proventia, BlackICE et RealSecure d'ISS
Date de la première version	27 février 2004
Date de la dernière version	–
Source(s)	Avis AD20040226 d'eEye digital security
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Proventia séries A, G et M ;
- BlackICE PC ou Server version 3.6 ;
- RealSecure Sentry, Guard ou Desktop 3.6 ;
- RealSecure Desktop, Network ou Server Sensor 7.0.

3 Résumé

Une faille a été identifiée dans les sondes d'ISS qui permet d'exploiter une vulnérabilité de type débordement de tampon. Cette dernière pourrait permettre à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sans authentification avec des privilèges élevés.

4 Description

Les produits d'ISS (Internet Security Systems) cités ci-dessus incluent systématiquement une sonde de détection d'intrusions parfois couplée à un pare-feu (BlackIce, Porventia).

Le code d'analyse du protocole SMB (Server Message Block), utilisé par les systèmes d'exploitation de Microsoft pour partager des ressources, comporte une faille qui peut être utilisée pour corrompre la mémoire.

Un seul paquet serait suffisant pour exploiter ce défaut.

5 Contournement provisoire

Filtrer les ports SMB (445/tcp ou encapsulé dans NetBIOS 137, 138/udp et 139/tcp) sur les pare-feux permet de limiter les risques à des attaques provenant de la même zone de sécurité (ce qui n'exclut pas les rebonds). Cette règle est, par ailleurs, recommandée de façon générale.

6 Solution

Mettre à jour en fonction des recommandations du vendeur :

- BlackICE :
http://blackice.iss.net/update_center/index.php
- RealSecure :
<http://www.iss.net/download/>

7 Documentation

- Avis AD20040226 de eEye digital security :
<http://www.eeye.com/html/Research/Advisories/AD20040226.html>
- Note de vulnérabilité du CERT/CC :
<http://www.kb.cert.org/vuls/id/150326>
- Avis de sécurité d'ISS :
<http://xforce.iss.net/xforce/alerts/id/165>

Gestion détaillée du document

27 février 2004 version initiale.