



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2003
N° CERTA-2003-AVI-083

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur Microsoft BizTalk

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-2003-AVI-083>

Gestion du document

Référence	CERTA-2003-AVI-083
Titre	Vulnérabilités du serveur Microsoft BizTalk
Date de la première version	12 mai 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS03-016
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 ;
- injection de code SQL.

2 Systèmes affectés

- Microsoft BizTalk Server 2000 ;
- Microsoft BizTalk Server 2002.

3 Résumé

Deux vulnérabilités ont été découvertes dans le serveur Microsoft BizTalk.

4 Description

Microsoft BizTalk Server est un produit destiné aux entreprises qui souhaitent intégrer diverses applications et partenaires dans leur traitement d'informations.

Deux vulnérabilités ont été découvertes sur ce produit.

La première vulnérabilité ne concerne que la version Microsoft BizTalk Server 2002. Il est possible d'échanger avec BizTalk Server 2002 des documents au format HTML. Une vulnérabilité de type débordement de mémoire a été découverte dans le composant chargé de recevoir les documents HTTP, et permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le serveur BizTalk.

Le transfert de documents au format HTTP n'est pas mis en place par défaut, et doit être explicitement demandé durant l'installation. De plus, le code sera exécuté avec les droits du serveur IIS. Si ce dernier est installé sous un compte d'utilisateur, les permissions seront limitées à celle de l'utilisateur.

La deuxième vulnérabilité concerne les versions 2000 et 2002 du serveur BizTalk. BizTalk Server permet aux administrateurs d'organiser des documents via une interface web (*DTA - Document Tracking and Administration*). Dans certaines pages de cette interface, il est possible d'injecter du code SQL qui sera exécuté sur le serveur.

Les utilisateurs par défaut de l'interface DTA ne sont pas des utilisateurs SQL privilégiés. En effet, pour pouvoir utiliser cette interface, il suffit à un utilisateur de faire partie du groupe *BizTalk Server Report Users*.

5 Solution

Appliquer le correctif fourni par Microsoft (cf. section Documentation).

6 Documentation

Avis de sécurité Microsoft MS03-016 :

<http://www.microsoft.com/technet/security/bulletin/MS03-016.asp>

Gestion détaillée du document

12 mai 2003 version initiale.