

# Microsoft Biztalk Server DTA vulnerable to SQL injection

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-05/0011.html>

---

**From:** Cesar (*cesarc56\_at\_UOL.COM.AR*)

**Date:** 05/05/03

Date: Mon, 5 May 2003 17:26:28 -0300  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

## Security Advisory

Name: Microsoft Biztalk Server Document Tracking and Administration vulnerable to SQL injection

System Affected : BizTalk Server 2000 and BizTalk Server 2002

Severity : High

Remote exploitable : Yes

Author: Cesar Cerrudo.

Date: 05/05/03

Advisory Number: CC040302

## Legal Notice:

This Advisory is Copyright (c) 2003 Cesar Cerrudo. You may distribute it unmodified and for free. You may NOT modify it and distribute it or distribute parts of it without the author's written permission. You may NOT use it for commercial intentions (this means include it in vulnerabilities databases, vulnerabilities scanners, any paid service, etc.) without the author's written permission. You are free to use Microsoft bulletin's details for commercial intentions.

## Disclaimer:

The information in this advisory is believed to be true though it may be false.

The opinions expressed in this advisory are my own and not of any company. The usual standard disclaimer applies, especially the fact that Cesar Cerrudo is not liable for any damages caused by direct or indirect use of the information or functionality provided by this advisory. Cesar Cerrudo bears no responsibility for content or misuse of this advisory or any derivatives

thereof.

#### Overview:

Microsoft Biztalk Server is a Microsoft product for business–process automation and application–integration both within and between businesses. BizTalk Server provides a powerful Web–based development and execution environment that integrates loosely coupled, long–running business processes, both within and between companies.

BizTalk Server features include integration among existing applications; the definition of document specifications and specification transformations; and the monitoring and logging of run–time activity. The server provides a standard gateway for sending and receiving documents across the Internet, as well as providing a range of services that ensure data integrity, delivery, security, and support for the BizTalk Framework and other key document formats.

Microsoft BizTalk Server provides the ability for administrators to manage documents via a Document Tracking and Administration (DTA) web interface. A SQL Injection vulnerability exists in some of the pages used by DTA that could allow an attacker to send a crafted URL query string to a legitimate DTA user and to execute a malicious embedded SQL statement in the query string.

#### Details:

BizTalk Document Tracking and Administration is a stand–alone Web application that you can use to view interchanges and documents that you configured to be tracked in Microsoft BizTalk Server. Biztalk Server uses SQL Server as a backend database server.

Only members of Windows administrators or BizTalk Server Report Users local groups are granted by default to use Biztalk Document Tracking and Administration user interface and view tracked documents.

The web application authenticate users by Windows authentication, the credentials are also used to authenticate to SQL Server. The web application is located at:

## NT-Bugtraq: Microsoft Biztalk Server DTA vulnerable to SQL injection

<http://server/biztalktracking/>

There are two ASP pages on the web application that connect from server side to SQL Server that are vulnerable to SQL injection:

<http://server/biztalktracking/rawdocdata.asp>

<http://server/biztalktracking/RawCustomSearchField.asp>

Exploits:

[http://server/biztalktracking/rawdocdata.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.xp\\_cmdshell 'any OS command'--](http://server/biztalktracking/rawdocdata.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.xp_cmdshell 'any OS command'--)

[http://server/biztalktracking/RawCustomSearchField.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.xp\\_cmdshell 'any OS command'--](http://server/biztalktracking/RawCustomSearchField.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.xp_cmdshell 'any OS command'--)

or

[http://server/biztalktracking/rawdocdata.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.sp\\_grantlogin 'domain\attacker'--](http://server/biztalktracking/rawdocdata.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.sp_grantlogin 'domain\attacker'--)

[http://server/biztalktracking/RawCustomSearchField.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.sp\\_grantlogin 'domain\attacker'--](http://server/biztalktracking/RawCustomSearchField.asp?nDocumentKey=1,@tnDirection=1;exec master.dbo.sp_grantlogin 'domain\attacker'--)

...etc.

There are others ASP and HTML pages in the Web application that connect to SQL Server with activex components from client side that are also vulnerable to SQL injection. But when a user access these pages a warning message is displayed by Internet Explorer with default security settings for Intranet Zone: "This page access data on another domain. Do you want to allow this" Making the exploitation harder without alarming the targeted administrators.

This vulnerability can be exploited through XSS or sending an administrator an HTML e-mail, etc. targeting the vulnerable server. Exploitation of this vulnerability allows an attacker to complete compromise SQL Server and could lead to further OS compromise.

NT-Bugtraq: Microsoft Biztalk Server DTA vulnerable to SQL injection

Workaround:

Edit ASP and HTML source files to filter malicious input.

Vendor Status :

Microsoft was contacted 02/14/03, we work together and Microsoft released a fix.

Patch Available :

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

---

UOL Sinectis – Mucha m&aacutes Internet  
<http://www.uol.com.ar>

oo  
Delivery co-sponsored by IP3 Inc.  
oo  
SECURITY QUESTIONS? We've got answers...Apply for a scholarship and become  
TICSA certified.

Do not miss your opportunity to discover solutions to what our participants have identified as their top 5 IT Security Challenges. You will return to work better prepared to put into place an effective security strategy utilizing the latest security tools, bookmarks and URL's.

<<http://www.ip3seminars.com>>

oo