

MWR InfoSecurity Security  
Advisory

Websphere MQ Security Exit  
Authentication Bypass  
Vulnerability

30<sup>th</sup> April 2007

MWR  INFOSECURITY

**CONTENTS**

<b>1</b>	<b>Detailed Vulnerability Description.....</b>	<b>5</b>
1.1	Introduction .....	5
1.2	Technical Background .....	5
1.3	Exploit Information .....	7
1.4	Dependencies .....	8
<b>2</b>	<b>Recommendations.....</b>	<b>9</b>
<b>3</b>	<b>References and Acknowledgements.....</b>	<b>10</b>

## Websphere MQ Security Exit Authentication Bypass Vulnerability

<b>Package Name:</b>	Websphere MQ
<b>Date:</b>	30 <sup>th</sup> April 2007
<b>Affected Versions:</b>	Websphere MQ 5.1 – 5.3 on Solaris are confirmed to be vulnerable Websphere MQ 6.0.0.0 on Windows is not vulnerable

**CVE Reference:** CVE-2008-1130

**Severity:** High Risk

**Local/Remote:** Remote

**Vulnerability Class:** Authentication Bypass

**Vendor Response:** The vendor has released a fix pack that addresses these issues.

**Exploit Details Included:** Yes (although no exploit code is provided)

**Affected OS:** Solaris (although others could also be affected)

### Overview:

The Websphere MQ service can be used to transfer messages between systems and applications. It is possible to protect the channels within the Queue Manager with a security exit which requires that an authentication check be passed before a connection can be established. A method of bypassing this authentication has been discovered which would enable unauthorised access to be gained.

### Impact:

The vulnerability could enable an attacker to bypass a security exit that has been applied to a channel. This would enable an attacker to gain full access to all queues defined within the queue manager with full read and write access. Additionally, an attacker could perform remote fingerprinting of the software, alter the Queue Manager configuration and potentially execute Operating System commands through the creation of an appropriate trigger process. The latter is dependent on the presence of a running trigger monitor process on the system.

### Cause:

The vulnerability arises from an error in the process for checking whether a connection has successfully passed the authentication check enforced by a security exit. A connection can be established to the Queue Manager if an authentication packet is not sent before the connection is established.

**Interim Workaround:**

The only workaround at the present time is to use network filtering to restrict access to Websphere MQ services to trusted IP addresses only. It is also possible that correctly deploying and mandating the use of SSL client certificates will prevent an attacker from accessing the channels that are protected by the Security Exit. IBM have released a fix pack that addresses this vulnerability.

**Solution:**

IBM has released the following fix Pack:

<http://www-1.ibm.com/support/docview.wss?rs=171&uid=swg27006037#1>

## 1 Detailed Vulnerability Description

### 1.1 Introduction

WebSphere MQ is an Enterprise level application that can be used to provide a unified platform for messaging within an organisation. IBM describes their technology as follows: -

“WebSphere MQ provides an award-winning messaging backbone for deploying your enterprise service bus (ESB) today as the connectivity layer of a service-orientated architecture (SOA).”

*Source: <http://www-306.ibm.com/software/integration/wmq/>*

Communication with MQ services can be achieved in a number of manners and the technology requires a feature rich API and extensions in order to integrate with an Enterprise environment.

### 1.2 Technical Background

#### Technical Introduction to MQ

The main component of a Websphere MQ instance is the Queue Manager. This is a process that manages the message queues and provides interfaces (known as channels) to the applications wishing to communicate with them. The Queue Manager can communicate using a number of protocols including IP and SNA (LU 6.2) amongst others.

MQ services on a given system can be detected by the presence of open TCP ports. By default, WebSphere MQ listens on TCP port 1414; however, it is often the case that other ports are used to run queue managers and an attacker would therefore be required to search for these services.

Queue detection required a handshake to be attempted on each open TCP port. A tool was written in-house and used to search for legitimate message queues by sending an MQ “INITIAL\_DATA” packet (the segment type was set to 01h in the Transmission Segment Header).

To connect to an instance of Websphere MQ it is necessary to establish communications with a specific channel. A channel is essentially a conduit through which communication with the message queues can occur. Therefore, it is necessary to know a valid channel on the remote system before connection can occur. A number of server connection channels are present by default and these will often be the first target of an attacker. In most cases the default channel “SYSTEM.DEF.SVRCONN” can be used to attempt attacks against the service.

If a legitimate MQ service is running on a port a valid MQ packet will be returned containing the name of the Queue Manager. Other possible responses could be error messages; for instance, stating the channel name was incorrect or that the Queue Manager was not available. This technique enables an attacker to identify the presence of a Queue Manager even when located on a port away from the default value.

## Security Exits

To prevent unauthorised communication with channels defined on a Queue Manager, it is possible to implement a security exit. This is a mechanism that enables a remote connection to authenticate to the Queue Manager. This provides a greater level of security than simply using the MCAUSER parameter and a number of products are on the market to provide such functionality.

If the channel is configured with a security exit the client will attempt authentication by passing a UID block that includes the username and password required for access. A WebSphere MQ network listener can be configured to support a security exit whereby an external program is used to perform the user authentication. If no exit is defined the listener will allow connections without authentication details being passed in the login packet. If an exit is defined, it is usually configured to check the username and password that have been passed. An exit can either be a proprietary solution or in-house custom written code.

## MQ Connection Process

When a connection to the MQ service is attempted a number of steps are involved. The first step involves an exchange of initial data which continues until the systems have agreed on parameters such as protocol version; heartbeat interval and sequence wrap value. At this stage, the remote queue manager also notifies the client whether authentication is required by setting the "Server Connection Security" bit. The initial data exchange can involve a number of packets being exchanged until suitable values have been agreed by the client and server.

Once this exchange of initial data has occurred the client will typically send an authentication packet to the server (those using the MQ APIs will do so by default). This will contain the authentication information required to access the channel. This packet will have the segment type set to 08h in the Transmission Segment Header (TSH). If the channel is configured with a security exit a Security Data packet should be returned with a segment type set to 06h. If the correct authentication details are not passed to the service a Status Data packet containing the error "Terminated by Remote Exit" will be returned and the communication will terminate.

## Vulnerability Details

A vulnerability was discovered such that an attacker could bypass the security exit by not sending the user authentication packet and proceeding directly to the connection request. On the affected systems this resulted in unauthorised access being gained to the protected channels.

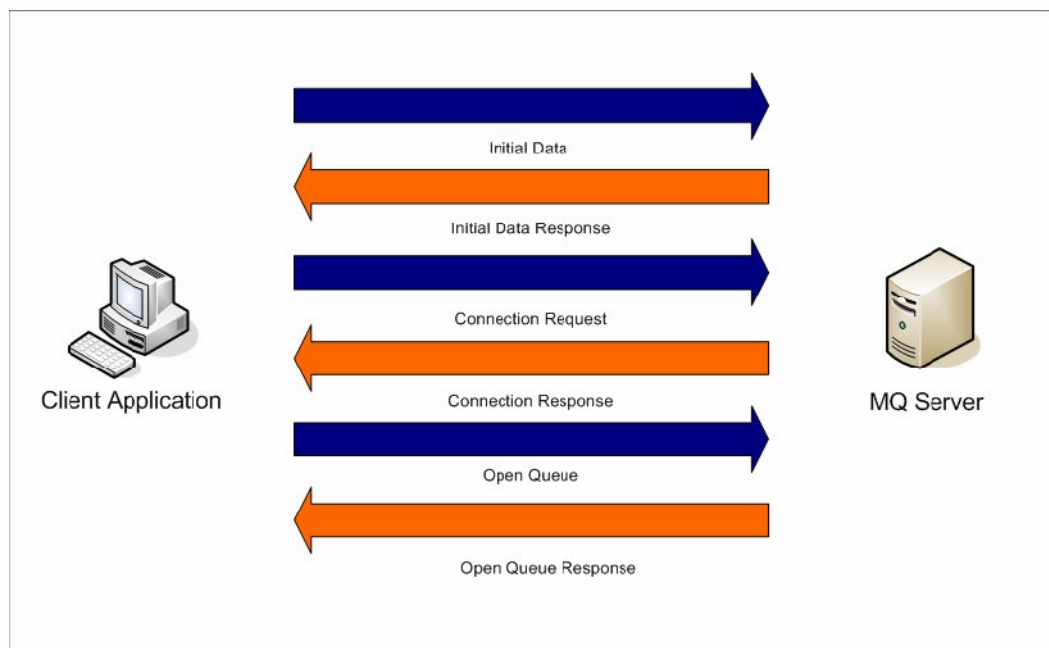
The sequence of packets required to gain access to an affected system is described in the Exploit Information section of this document. This vulnerability was confirmed on Websphere MQ versions 5.1, 5.2 and 5.3 on Solaris. This was reported to IBM's MQ team on 25<sup>th</sup> January 2007 and at the present time the public status of this issue is unknown. Version 6.0 of the software on the Microsoft Windows platform is confirmed not to be vulnerable although it is unknown whether any fixes were included in this version.

## Vulnerability Impact

An attacker capable of bypassing the authentication controls can gain full access to a protected channel. Depending on the configuration of the software this could result in a serious security breach. An attacker would be able to communicate with the Queues associated with the channel and this could result in the compromise of the confidentiality or integrity of the Queue data. Additionally, if an attacker were able to access the Command Server through the channel it would be possible to alter the configuration of the Queue Manager and so could potentially result in Operating System commands being executed.

### 1.3 Exploit Information

The security exit defined for a channel can be bypassed by using a modified connection process. Therefore successful exploitation requires a custom MQ client to be written to perform this bypass attack. Code to perform the attack will not be provided at the present time; however, the sequence of packets that can be used to gain access to a protected channel is included here: -



As can be observed, the authentication sequence is not attempted during the handshake. The result of this is such that the connection request is accepted and access is granted to the channel. This exploit does not enable GET and PUT restrictions applied to queues to be bypassed but if the channel has Command Server access it becomes possible to reconfigure the Queue Manager using PCF commands.

Exploitation of the test system was demonstrated by placing a message on a queue on the protected channel. This was possible on the MQ versions that were tested by MWR InfoSecurity.

#### 1.4 Dependencies

This vulnerability has been tested on Websphere MQ versions 5.1, 5.2 and 5.3 on a Solaris platform. It is possible that further versions of the software are vulnerable to this issue although testing conducted against version 6.0.0.0 (evaluation download) on the Windows platform was not vulnerable during the limited testing that was performed.

## 2 Recommendations

To resolve the issue it is important that the State Machine implemented by the software is reviewed. This should ensure that a Connection Request cannot be made until the user authentication has been completed. It is therefore recommended that the vendor perform investigations to establish the cause of the vulnerability and provide an appropriate resolution.

It is recommended that all users install any security patches released by the vendor in response to this issue.

### Interim Workaround

The use of a security exit is one of the most effective mechanisms for protecting an installation of Websphere MQ therefore the workarounds suggested must be viewed purely as temporary fixes for this specific issue. However, these mitigations are best practice and the implementation of these as part of the MQ environment's security model are highly recommended.

The suggested method of mitigation is the use of client SSL certificates to protect all access to channels. It is important that the SSL filtering is performed in a rigorous manner and that all trusted Certificate Authorities are removed from the MQ system except for those that are under direct control of the organisation.

Additionally, both network and host based traffic filtering controls could be implemented to protect access to the Queue Manager service on the affected hosts. This should be considered at both the packet filtering level and by the use of IPSec tunnels between hosts.



### 3 References and Acknowledgements

MWR InfoSecurity would like to thank Peter G Spera of IBM for facilitating the initial contact with the MQ team at IBM.

**MWR InfoSecurity**  
St. Clement House  
1-3 Alencon Link  
Basingstoke, RG21 7SB  
Tel: +44 (0)1256 300920  
Fax: +44 (0)1256 844083  
[mwrinfosecurity.com](http://mwrinfosecurity.com)