

MWR InfoSecurity Security  
Advisory

WebEx Remote Support  
Center

3rd April 2009



## Contents

<b>1</b>	<b>Detailed Vulnerability Description .....</b>	<b>5</b>
1.1	Introduction .....	5
1.2	Technical Background.....	5
1.3	Vulnerability Descriptions.....	7
1.3.1	Access Control Mechanisms	7
1.3.2	Identity Verification	8
1.3.3	Application Security Controls	9
1.4	Attack Scenarios.....	11
<b>2</b>	<b>Recommendations.....</b>	<b>12</b>
<b>3</b>	<b>References.....</b>	<b>12</b>

## WebEx Remote Support Center

<b>Package Name:</b>	WebEx Remote Support Center Application
<b>Date:</b>	2009-04-03
<b>Affected Versions:</b>	All client versions available prior to 6 <sup>th</sup> February 2008

<b>CVE Reference</b>	CVE-2009-1145
<b>Authors</b>	M. Ruks, L. Jennings
<b>Severity</b>	High
<b>Local/Remote</b>	Remote
<b>Vulnerability Class</b>	Access Control Bypass
<b>Vendor URL</b>	<a href="http://www.webex.com">www.webex.com</a>
<b>Version</b>	All client versions available prior to 6 <sup>th</sup> February 2008
<b>Vendor Response</b>	The vendor was contacted and has provided an updated version of the WebEx client. This was released on 6 <sup>th</sup> February 2008 and all customers should have been protected from this date.
<b>Exploit Details Included</b>	No

This document is intended to provide further information about security vulnerabilities previously identified in the WebEx Remote Support Center Application. The information included here should be used to identify how use of the service might impact on an organisation's security posture and how it can be ensured that its usage does not expose unnecessary risk. This document is not intended as a statement of MWR InfoSecurity's opinion about the security of this application, or of the service in general.

MWR InfoSecurity have liaised with the vendor to ensure that the issues that were identified were communicated to them in an appropriate and timely manner and that effective resolutions could be implemented.

### Overview:

The Remote Support Center application utilises the WebEx portal to provide a mechanism which allows remote assistance of users or the sharing of an application such as a PowerPoint presentation or browser session. The application is designed such that a designated Meeting Host can control a session which can potentially contain multiple users; the Meeting Host can then use their authority to request various actions. For example a Meeting Host can request control of a user's desktop, control an application, share the host's desktop or transfer files between systems. The application is designed such that users are prompted as to whether they will allow any actions requested by the Meeting Host. The effect of the vulnerability is such that

these controls could have been overridden and that all actions could have been taken without the permission of the user or of the Meeting Host.

**Impact:**

The vulnerabilities could have enabled an attacker to use the Remote Assistance application to control a user's desktop in an unauthorised manner. A number of weaknesses in the security model of the facility would have enabled an unauthorised user to join a "Support Center" session and gain control over other participating systems. The impact would be dependent on the privileges the logged on user had over their local system, but could have resulted in extended control being gained over users' systems or applications.

**Cause:**

The principle vulnerability arose from incorrect session state handling within the "Support Center" application. The ActiveX controls did not correctly maintain state, and so the controls could be overridden. This resulted in the ability to bypass user responses and gain control of functions within the application in an unauthorised manner.

**Interim Workaround:**

All customers would have been prompted to update their WebEx client when using the online service and therefore no workaround is required.

**Solution:**

The vendor has provided a resolution to the issue although this has not been tested by MWR InfoSecurity. All customers should have received the updated version of the client whilst using the WebEx service after 6<sup>th</sup> February 2008.

## 1 Detailed Vulnerability Description

### 1.1 Introduction

WebEx provide online portal solutions for a variety of uses, including the hosting of meetings, application sharing and remote support. One of the solutions that is currently offered is for providing Remote Support to users. This allows administrators to invite users to a meeting which enables them to observe and control a user's applications and desktop. A variety of services are offered through this facility to enable effective and efficient remote support; for example, file transfers and the ability to observe and interact with a user's desktop.

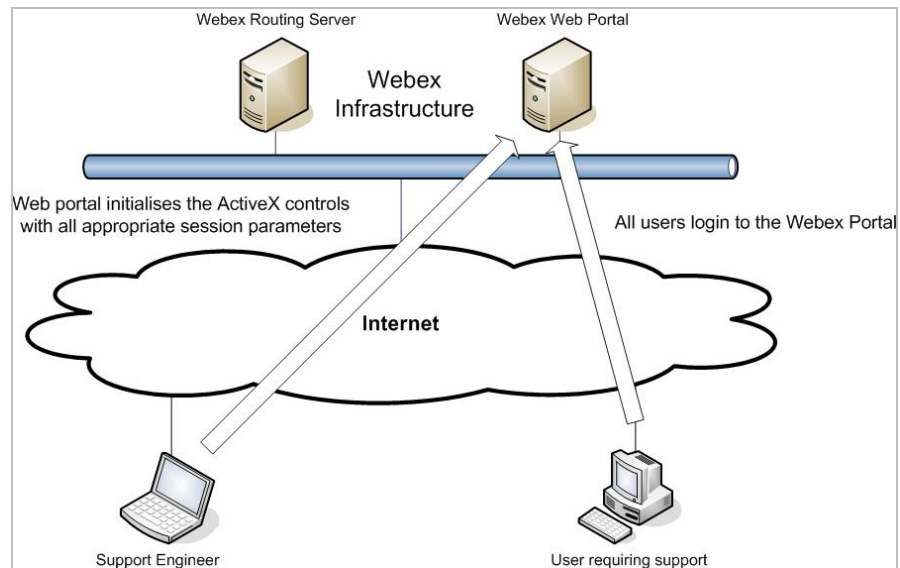
A number of security features have been implemented to protect meetings from various threats. Access to a meeting requires a Meeting Number that must be protected to prevent unauthorised access to a session. Additionally, the remote support facilities are designed such that a user has the ability to deny all requests made by the "Meeting Host" as well as being able to regain control over their desktop or application.

However, analysis of the application revealed that the security controls did not function as expected; the vulnerability that arises from this are described below. Given the nature of the WebEx service this document only illustrates how the issue could potentially have affected users. No technical details concerning the methods for completing an attack are provided and no comment is made about the remedial actions implemented by WebEx to resolve the issues.

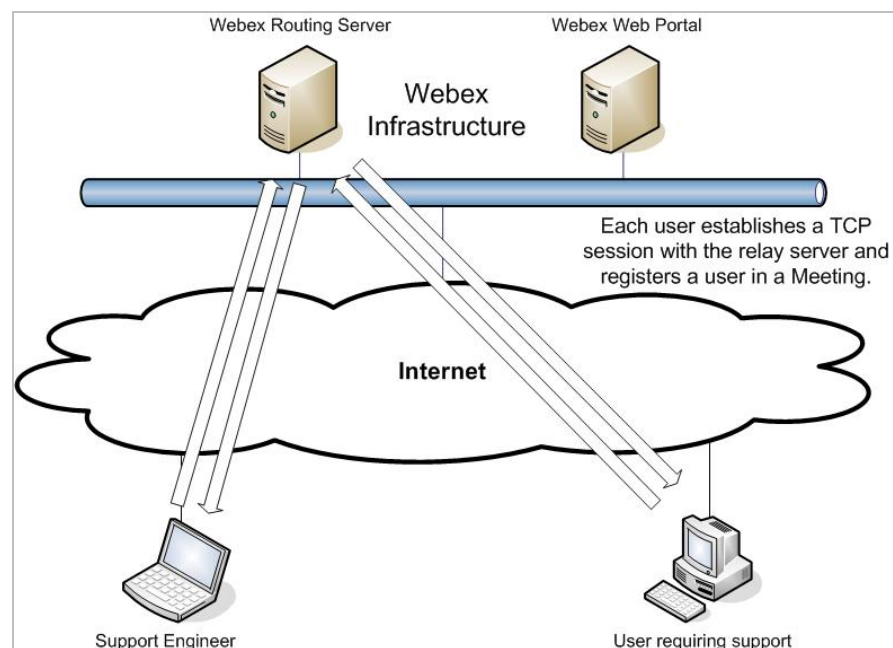
### 1.2 Technical Background

The following brief outline of the architecture of the service provided by the Webex Remote Assistance Center is provided as a technical background to the security vulnerability that was identified. It should be noted that this description includes an overview of the operation of the service rather than technical details. This discussion relates to the WebEx service prior to the resolution of this issue and therefore aspects of the following discussion may have been rendered obsolete by the recent update.

The Remote Support application is provided through a web browser and uses the WebEx infrastructure to host the session. A basic diagram of the infrastructure used to provide the solution is included here (please note: all terms used in this section are descriptions applied by MWR InfoSecurity and may not be those utilised by WebEx):-



The diagram above highlights how a Meeting Host will initiate a Remote Support session using the WebEx web application front end. This process uses the HTTPS protocol and operates in a similar fashion to other enterprise level web based applications. The web portal access is used to setup a new meeting and generates two new security tokens, the Meeting ID and the Meeting Key. The Meeting Key is the “password” for the session and is required to join the Remote Support session. These parameters (and a large amount of additional data) are used by the web application to initialise an ActiveX control for a user’s session. Each user who logs into the session, including the Meeting Host and any other participants, uses an ActiveX control that is initialised through the web portal to communicate with a WebEx routing server. A basic diagram of the architecture used to support the session is included here: -



As can be observed, the routing server allows all users to communicate with the other participants of a Meeting by accepting inbound data and forwarding it on to the correct host. In this manner users can directly interact with each other even when located on separate network segments which could be protected with network layer security controls. All traffic passes through the WebEx relay and is routed by a custom daemon to the appropriate system via an established TCP session. The network traffic is handled exclusively by the user's ActiveX control and communicates with the WebEx system using a custom protocol.

The network protocol is designed to ensure that all connections to the WebEx relay are authenticated (using the Meeting ID and Meeting Key) and provides a keep-alive mechanism to maintain the state of the TCP connection for each participant. No further technical details of the operation of this part of the service are necessary for this discussion.

Once a meeting has been initiated and participants have successfully connected it is possible to request various actions using a dashboard built into the ActiveX control. These requests are routed to a specific user based on the Meeting ID, Meeting Key and user number to which the request is addressed.

### 1.3 Vulnerability Descriptions

A number of security issues were identified in the Remote Support facility and should be understood by users of the service. The impact of these issues varies and can expose users to different risks.

#### 1.3.1 Access Control Mechanisms

The security of a meeting within WebEx is protected by two parameters that are assigned when a session is initiated. These are the Meeting ID and Meeting Key and act as individual references to the session that is in progress. The Meeting ID is a unique reference for the session and is a number that increments by 1 for each new meeting that is started. The Meeting Key is a 9 digit number that is generated by WebEx and is the number that is used by delegates to join a meeting.

To participate in the meeting both of these values are required; however, if a valid Meeting Key is presented to the WebEx portal by a user the Meeting ID will be provided by the application. The security of any session is therefore ultimately dependent on the secrecy of the Meeting Key and therefore it is important that this be given suitable protection by any user of the service.

The WebEx application provides users with the ability to invite people to a meeting by creating an email that can be sent to an email address of their choice. The content of one of these emails is shown below and includes the Meeting Key in the link that is contained within it: -

```
Hello USERNAME,  
  
I would like to invite you to join a Remote Support Session with me. Please click  
the link below to join the session.  
  
https://URL/file?I=617972530  
  
Regards,  
SENDER  
  
http://www.webex.com  
Bringing the support to you (TM)
```

If the email is sent to a user the Meeting Key (highlighted in bold in the example above) will be sent in clear text and could therefore be intercepted by any malicious party capable of viewing a user's network traffic. This party could be located at any point on the Internet that the mail passes through. With knowledge of the Meeting Key it would then be possible to attempt the attacks against the Remote Support facility as described in the following section.

All Remote Support users should be made aware of the importance of securing this data to protect their WebEx sessions from unauthorised persons.

### 1.3.2 Identity Verification

As described previously, a user will be invited to use the Remote Support facility by a communication from the Meeting Host, whether via email, telephone call or some other mechanism. It is therefore important that a user can trust that the request to administer their PC is from a legitimate and authorised source.

However, the WebEx application does not include any user verification features and therefore a user cannot be certain that the host of a meeting is a genuine representative. The only reference to the remote user is the name they are required to specify either when enabling a meeting or when logging in as a participant. However, this can be set to an arbitrary value and is not unique for every user registered with WebEx.

The Remote Support application is therefore a potential target for Social Engineering attacks and could be used by an attacker to trick a user into accessing the WebEx application. This could be achieved by targeting them with a Phishing link type email or a telephone call. The attacks that are possible due to the lack of identity verification are described later in this document.

### 1.3.3 Application Security Controls

The Remote Support software provides the ability for a user and administrator to perform a number of operations through an ActiveX control installed on their system. The control offers a number of facilities including the ability to gain control of a remote application or desktop or to transfer files between the systems.

The application controls are designed to enable the person hosting the meeting to make requests to control the systems used by other meeting participants with those individuals being limited to using the chat facilities. The security model is designed such that all requests that are made by a host must be accepted by the user before any access is granted.

A number of issues associated with the service were identified during the evaluation of the service (please note that these have not been re-investigated since the vendor resolved the session state handling issue). These issues are described here to enable users to identify how the use of the service could impact on their information security policy and processes.

- Single Link Authentication – it is common for users to be invited to a meeting by providing them with the Meeting Key which enables them to join the session from the main WebEx website. Once the key has been entered a user can then enter their name and the email address that they wish to be identified by within the application. If they do not have the WebEx ActiveX control installed they will be prompted to install it; if it is present, the application will automatically start. However, it was discovered that this process could be triggered by simply accessing a single URL in a browser; consequently, clicking a link would take a user with the ActiveX control already installed straight into a remote support session. This could therefore provide an attacker with the ability to send a Phishing link to a user which, when it was clicked, would automatically drop them into a meeting that had previously been established.
- Proxy Server Bypass – the operation of the application can be divided into two parts. The first is an interaction with the WebEx servers using the HTTPS protocol and enables a user to authenticate and join a meeting. The web application then enters the second stage of its operation in which it passes a large amount of information to the user's ActiveX control which then communicates with WebEx using a proprietary TCP protocol. Users must disable any browser proxies in order to communicate with the WebEx protocol (at least for the WebEx relay server IP addresses). If sufficiently granular proxy controls cannot be implemented this could represent a security risk or operational issue for an organisation using the service.

A number of vulnerabilities were also identified which were associated with the manner in which the ActiveX controls responded to unexpected traffic. Full technical details of these vulnerabilities will not be provided, however, they are outlined below: -

- Application Control Bypass – the WebEx facility enables the meeting host to control either a user’s desktop or a single application running on their system. The ability to control a single application could potentially be used to prevent a remote support engineer from gaining full control over a system whilst enabling them to diagnose a support issue. However, investigation of this functionality revealed that the controls in place to restrict access to a single application were not correctly implemented. For example, control over an instance of Internet Explorer (IE) could be used to spawn new applications using IE’s own functionality; IE could be used to spawn a new Windows Explorer process which would grant file system access under the context of the remote user’s logon account. This highlights that the WebEx application does not enforce controls on the applications and processes that can be controlled by the remote user but instead places partial responsibility for security on the controls within the application that is being shared.
- Unauthorised Application Control – the WebEx remote support application provides a Meeting Host with the ability to perform a number of actions. Each request that is made for one of these actions prompts a user to allow control to be taken by the Meeting Host. However, it was demonstrated that a number of attacks were possible against these features and this included the ability to alter a user’s response before it was received by the Meeting Host’s ActiveX control. This could be used to change a negative response to a request for access to a positive response. Additionally, it was also possible to control the relevant application, desktop or file sharing facility without prompting the user. Each of these attacks would result in the Meeting Host taking control of the file sharing facility, a user’s application or their desktop without their authorisation.
- Mouse Click Deactivation – the application is designed such that a local user can regain control of their desktop by clicking the mouse at any time. However, testing revealed that control was only regained when a signal was passed to the ActiveX control of the user currently in control. When this occurs, the user in control is responsible for passing control back to the local user. Therefore, a user’s requests could simply be dropped before they were received by the host’s ActiveX control ensuring the mouse click would never be registered. It was demonstrated that this technique could be used to ensure a meeting host could retain control over a user’s desktop without them being able to regain control. This could be used in conjunction with the attacks described previously to maintain control over a user’s desktop whilst malicious actions were performed.
- Unauthorised Control of Meeting Host – a Meeting Host could issue requests to a user but not vice versa. However, it was discovered that it was possible to send messages to the Meeting Host such that control of their desktop was requested and honoured. This could result in a user gaining unauthorised control of the Meeting Host’s system and preventing them from regaining control of it.

## 1.4 Attack Scenarios

Testing highlighted that a number of significant security weaknesses were present in the WebEx Remote Support facility. The issues that were identified would enable a malicious user to perform attacks against WebEx users in a number of ways. A number of potentially viable attack scenarios are described here: -

- Legitimate Support Person – given sufficient technical knowledge a legitimate remote support engineer could utilise the application to gain control of a user’s system and perform actions on it with the privileges of the logged on user. This could potentially provide them with the opportunity to view sensitive user data or attack other systems belonging to that user.
- Malicious Support Technician – a person masquerading as a genuine remote support engineer could use the application to control a user’s desktop PC if that user could be tricked into accessing the service. This could be achieved due to the lack of identity verification within the product and could result in the exposure of a user’s system as described above.
- Phishing Link Attack – a remote attacker could craft a link that could be sent to known WebEx users by email or Instant Messenger, or placed on a third party website. If a user with the ActiveX control already installed clicked on such a link they could unwittingly join a remote support session where a malicious user could take control over their PC.
- Meeting Host Attack – if a Meeting Host were to invite users to a session it would be possible for a malicious user to gain control of the Meeting Host’s system. If an administrative user were to host the meeting this could allow the malicious user to gain control of systems under the context of a highly privileged user account.

## 2 Recommendations

The vendor has responded to the issues described in this document and has updated the service to include controls which prevent the attacks discussed within this document. Whilst the robustness of these controls has not yet been confirmed by MWR InfoSecurity, the vendor released a security advisory on February 6<sup>th</sup> 2008 which confirmed that the appropriate actions had been taken to resolve the issues in the software.

Nevertheless, a number of recommendations are made in light of the issues that were previously identified to limit the risk associated with the use of this service. These recommendations are security best practice and in no way reflect upon the security of the WebEx service at the present time.

- The Meeting Key should only be communicated over secure channels.
- A method of confirming the identity of the Meeting Host and participants should be agreed.
- All participants should be logged onto their desktop PCs with minimal privileges.
- If a single application is to be shared it should be tested to ensure it cannot be used to spawn further processes.
- Users should be provided with advice about how to respond to any instances whereby they believe unauthorised activity is occurring through their session.

## 3 References

The vendor's advisory information can be found at the following location: -

<http://www.webex.com/companyinfo/webex-security-advisory-webx-07-11-28.html>

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)