

MWR InfoSecurity Security  
Advisory

National Rail Live Enquiries  
Departure Board Gadget  
Vulnerability

24<sup>th</sup> April 2008

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	Overview of Vulnerability.....	5
1.4	Exploit Information .....	6
1.5	Dependencies .....	7
<b>2</b>	<b>Recommendations.....</b>	<b>8</b>

## National Rail Live Enquiries Departure Board Gadget Vulnerability

<b>Package Name:</b>	National Rail Live Departure Board Windows® Vista™ Gadget
<b>Date:</b>	2nd October 2007
<b>Affected Versions:</b>	Confirmed in Version 1.0

CVE Reference	Not Yet Assigned
Author	R Dominguez Vega
Severity	High Risk
Local/Remote	Remote
Vulnerability Class	Script Injection / Remote Code Execution
Development Company	National Rail Enquiries <a href="http://www.nationalrail.co.uk/">http://www.nationalrail.co.uk/</a>
Developer Response	A fix has been implemented for version 1.1  National Rail Live Enquiries Departure Board Gadget upgrade can be found in the following location <a href="http://gallery.live.com/LiveItemDetail.aspx?li=ae90e44-18cf-4246-b1d9-4ab83e0e13db">http://gallery.live.com/LiveItemDetail.aspx?li=ae90e44-18cf-4246-b1d9-4ab83e0e13db</a>
Exploit Details Included	Yes
Application Language	HTML, JavaScript and VBScript

### Overview:

The Windows Vista operating system includes the “Windows Sidebar”. This new feature allows users to display ‘gadgets’ on the Sidebar and on the Windows desktop. Gadgets are small applications which can be very flexible in design and function. They are managed by the Windows Sidebar and can be used for many purposes. The range of their functionality and sophistication is dependent upon the developer’s creativity and skill. Windows Vista includes various gadgets by default, such as a calendar, calculator, currency converter, etc.

### Impact:

The National Rail Live Departure Board gadget has been identified as being vulnerable to a script injection attack that could potentially allow remote attackers to execute commands on the target system. An attacker successfully exploiting this vulnerability could execute arbitrary commands in the context of the current logged in user.

The National Rail Live Departure Board Sidebar gadget vulnerability is present because of a lack of sufficient sanitisation on arguments passed from the web server to the Sidebar gadget application.

### Cause:

Exploitation of this vulnerability is possible because the National Rail Live Departure Board Sidebar gadget does not properly sanitise parameters that are passed to it. If a script is passed to the Sidebar gadget from an attacker capable of intercepting traffic between the gadget and the web server, the script is injected into the gadget and therefore is executed.



**Interim Workaround:**

Remove the gadget from the sidebar until a fix is provided. Communications between the server and the gadget should be correctly protected by use of SSL; when correctly implemented this will minimise the risk of an attacker manipulating the traffic.

**Solution:**

The vendor has addressed this vulnerability and implemented a fix in version 1.1. This version has yet to be tested.

National Rail Live Enquiries Departure Board Gadget upgrade can be found in the following location:-

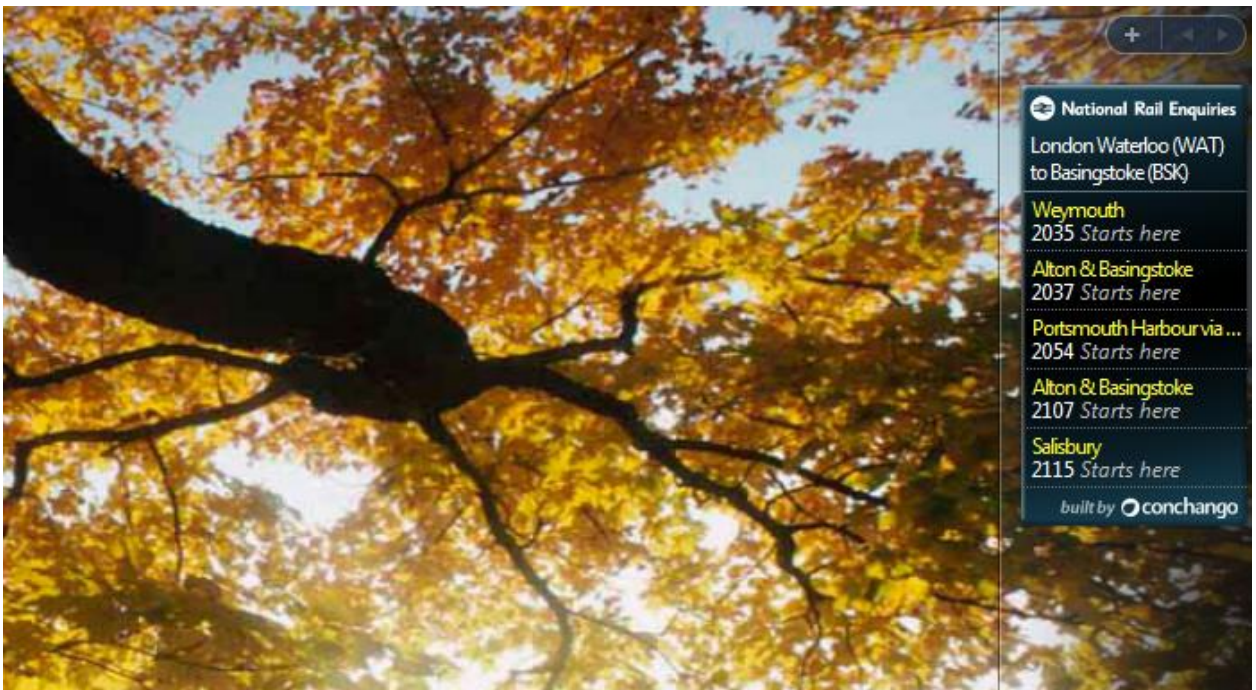
<http://gallery.live.com/LiveItemDetail.aspx?li=acf90e44-18cf-4246-b1d9-4ab83e0e13db>

## 1 Detailed Vulnerability Description

### 1.1 Introduction

The National Rail Live Departure Board Sidebar gadget provides users with the ability to view real time train departure boards for all main railway stations. The gadget allows users to choose a “Start Station” and a “Destination Station” in order to provide them with the most up to date live departure information for their chosen trip.

The screen shot below shows the Live Departure gadget running on the Sidebar: -



### 1.2 Technical Background

Windows Vista includes the “Windows Sidebar”. This new feature allows users to display ‘gadgets’ on the sidebar and on the Windows desktop. Gadgets are small applications which can be very flexible in design and function. They are managed by the Windows Sidebar and can be created by any Windows Vista user with moderate programming skills.

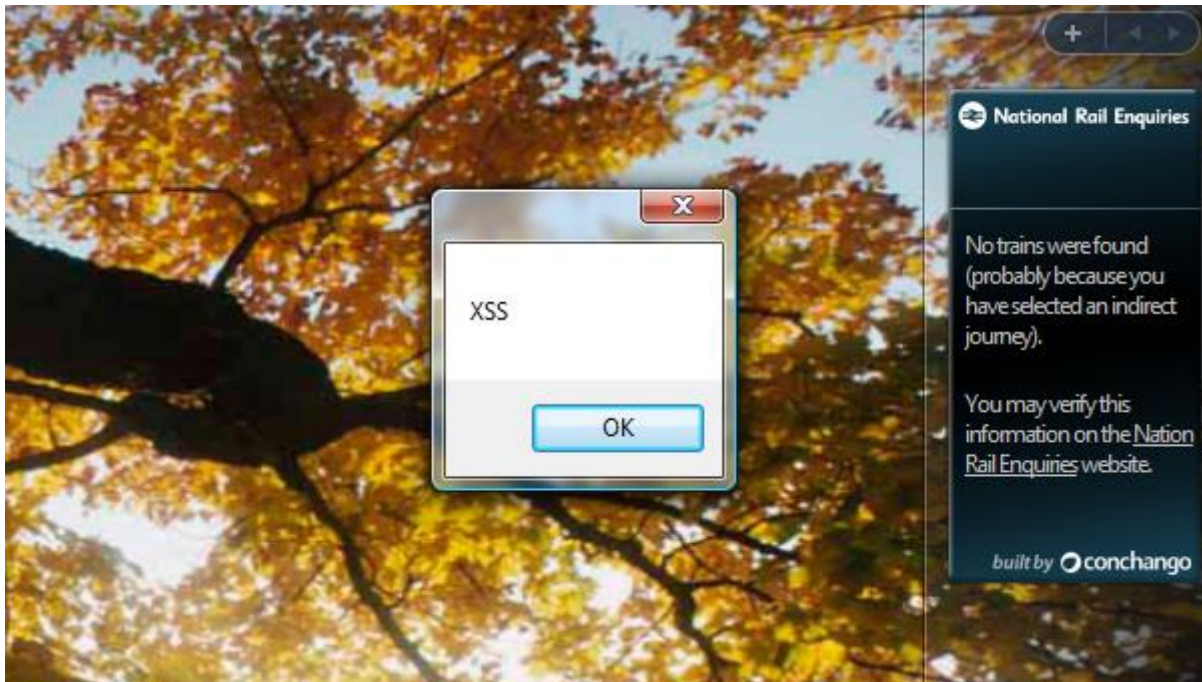
Gadgets can include HTML pages, XML files, CSS, JavaScript or VB code. This flexibility, when taken with the ability to use ActiveX and the gadgets’ APIs, makes the development of new gadgets very attractive for both Windows Vista users and potential attackers.

### 1.3 Overview of Vulnerability

The National Rail Live Departure Board gadget requests information from a web server, which responds to the gadget with live departure board information for the user’s chosen rail journey. An attacker capable of intercepting the web server response to the gadget request

could modify that response such that a script was injected and then run on the user's system. The injected script would run under the privileges of the currently logged in user

A screenshot of a JavaScript alert box being rendered after the web server response had been modified is included here: -



## 1.4 Exploit Information

It was possible to construct a proof of concept arbitrary remote code execution attack. This could be used as the basis of an attack which gained access to a user's machine at the privilege level at which they were logged on.

As a proof of concept, one simple example of executing commands via this attack is outlined below.

An attacker capable of intercepting the traffic between the National Rail Live Departure Board gadget and the remote web server which provides the gadget with departure information, could inject the following script into the body area of the response returned by the web server: -

```
<script SRC='vbscript:System.Shell.execute("cmd.exe", "/k ipconfig")'>
```

In this case this would result in the "ipconfig" command being executed on the user's system. However, an attacker could alter this code to execute commands of their choosing which, depending on the logged on user's privileges, could result in the remote compromise of the target system.

## 1.5 Dependencies

For this attack to be exploited an attacker would need to be able to intercept and modify network traffic between the remote web server supplying the departure information and the targeted user.

## 2 Recommendations

The following security measures are recommended to enhance the security of gadgets by validating the data received and securing the channel over which the data is transmitted.

- Transmission channel encryption - it is recommended that gadgets should use secure protocols (such as SSL) when receiving any data, even if that data is from what is perceived as a trusted source. This will prevent an attacker who is able to intercept the data from reading or manipulating this data. This technique does, of course, rely on a gadget correctly checking certificates presented.
- Source information validation - it is also recommended that the source from which the gadget obtains information is validated such that only data from specific sources can be processed and any data received from an unknown source is rejected.
- Input validation - it is recommended that the gadget be designed to correctly validate the data received from the server. This should include a white-listing function that only accepts the types of data required by the gadget.
- Server side issues - it is also recommended that the responses returned by a server, should only provide that information which is specifically required by the gadget, rather than returning complete HTML web pages. This would limit an attacker's chances of injecting scripts into the server response.

The article "Inspect Your Gadget", written by Michael Howard and David Ross is recommended reading and includes examples of secure gadget development. This article can be found at:-

<http://msdn2.microsoft.com/en-us/library/bb498012.aspx>

The whitepaper "Considerations for the Secure Rollout of Sidebar Gadgets in Windows Vista", written by Rafael Dominguez Vega is also a recommended reading. This whitepaper can be found at:-

[http://www.mwrinfosecurity.com/publications/mwri\\_sidebar-gadgets\\_2007-09-25.pdf](http://www.mwrinfosecurity.com/publications/mwri_sidebar-gadgets_2007-09-25.pdf)

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)