



#### Buffer Overflow:

The vulnerability specifically exists in the 'apply.cgi' handler of the HTTPd running on the internal interfaces, including the by default the wireless interface. This handler is used by many of the configuration pages to perform the configuration management of the router.

If an unauthenticated remote attacker sends a POST request to the apply.cgi page on the router with a content length longer than 10000 bytes, an exploitable buffer overflow may occur.

Exploitation of this vulnerability requires that an attacker can connect to the web management port of the router. The HTTPd is running by default but is only accessible via the LAN ports or the WLAN (wireless LAN). An attacker who can associate via the wireless interface to the network running a vulnerable HTTPd could send an exploit from a wireless device, and so not require direct physical access to an affected network. Additionally, if the HTTPd is configured to listen on the WAN (Internet) interface, this vulnerability would be exploitable remotely over the Internet.

On some versions of the WRT54G firmware the buffer used to store the POST input, 'post\_buf', is before a structure in memory containing pointers to the 'mime\_handlers' structure, which contains function pointers for handling the various types of input. By overwriting this structure so some function pointers point into post\_buf, it is possible to execute arbitrary commands. Overwriting these values with nulls will prevent access to the HTTPd on the system until the router is restarted. Overwriting these values with 'garbage' values will cause the HTTPd to crash but it will be restarted by a system monitoring process within 2 minutes, allowing multiple exploitation attempts.

Although authentication checks are performed on access to this page, the code which reads in the buffer is executed even if authentication fails, so as to clear the input buffer from the client before returning an error message. This may allow an unauthenticated user to exploit the vulnerability.

Remote exploitation of a buffer overflow vulnerability in multiple versions of the firmware for WRT54G wireless router may allow unauthenticated execution of arbitrary commands as the root user.

#### Authentication Bypass:

Remote exploitation of a design error in the upgrade.cgi component of Linksys WRT54G wireless router may allow unauthenticated modification of the router firmware.

The vulnerability specifically exists in the "POST" method of the upgrade.cgi handler. The HTTPd running on the internal interfaces, including by default the wireless interface, does not check if authentication has failed until after data supplied by an external user has been processed. The upgrade.cgi handler allows a user to upload new

firmware, which contains the operating system and applications, into the non-volatile memory of the router.

If the user is authenticated, the router will then restart, and the new firmware will be loaded. If the user is not authenticated, they will receive an error page when they attempt to upload a new firmware without supplying authentication and the router will not reboot. The firmware will be saved, but will not take effect until the next time the router restarts.

Successful exploitation of this vulnerability would allow an unauthenticated user the ability to completely compromise the affected router, by installation of an arbitrary firmware. As the source code and tools for compiling the firmware are available from the vendor, an attacker could simply rebuild the firmware and add the extra functionality. Exploitation of this vulnerability would require that an attacker connect to the web management port of the router. The HTTPd is running by default but is only accessible via the LAN ports or the WLAN (wireless LAN). For the uploaded firmware to be enabled, the router must be restarted.

#### Authentication Bypass:

The vulnerability specifically exists in the 'POST' method of restore.cgi handler. The HTTPd running on the internal interfaces, including by default the wireless interface, does not check if authentication has failed until after data supplied by an external user has been processed. The restore.cgi handler allows a user to upload a new configuration into the non-volatile memory of the router. If the user is authenticated, the router will then restart, and the new configuration will be loaded.

If the user is not authenticated, they will receive an error page when they attempt to upload a new configuration without supplying authentication and the router will not reboot. The settings the user set will be saved, but will not take effect until the next time the router restarts.

Successful exploitation of this vulnerability would allow an unauthenticated user the ability to modify the configuration of the affected router, including the password. This could allow firewall rules to be changed, installation of a new firmware with other features, or denial of service. Exploitation of this vulnerability would require that an attacker can connect to the web management port of the router. The HTTPd is running by default but is only accessible via the LAN ports or the WLAN (wireless LAN). A mitigating factor is that if the firmware settings are saved by a process on the router before the server is reset, the saved settings will overwrite the settings uploaded by the attacker.

An attacker who can associate with a network running a vulnerable HTTPd could send an exploit from a wireless device to reset the password on the device and enable the remote management port, allowing continued access from the Internet.

## Securiteam: [NEWS] Linksys WRT54G Router Multiple Vulnerabilities (Buffer Overflow, Multiple Authentication Bypass,

Remote exploitation of a design error in the 'restore.cgi' component of Linksys WRT54G wireless router may allow unauthenticated modification of the router configuration.

### Authentication Bypass:

Remote exploitation of a design error in multiple versions of the firmware for Cisco Systems Inc.'s Linksys WRT54G wireless router may allow unauthenticated modification of the router configuration.

The vulnerability specifically exists in the 'ezconfig.asp' handler of the HTTPd running on the internal interfaces, including by default the wireless interface. This handler is used by the 'ezSetup' to perform the initial setup of the router.

### Vulnerable Code:

```
struct mime_handler mime_handlers[] = {
//{{ "ezconfig.asp", "text/html", ezc_version, do_apply_ezconfig_post,
do_ezconfig_asp, do_auth },
/*Modified by Daniel(2004-09-06);*/
{ "ezconfig.asp", "text/html", ezc_version, do_apply_ezconfig_post,
do_ezconfig_asp, NULL },
```

The 'auth()' method for this page does not contain an authentication initialization function. As the authentication initializer (do\_auth) was removed, no check is made when requesting the page. If the auth\_fail flag was set for any reason, this call will fail. The code which sets the auth\_fail flag is shown below. When the HTTPd starts, the value of auth\_flag defaults to 0.

### Vulnerable Code:

```
if (handler->auth) {
handler->auth(auth_userid, auth_passwd, auth_realm);
auth_fail = 0;
if (!auth_check(auth_realm, authorization))
auth_fail = 1;
}
```

The request returns an encrypted version of the configuration information, however the encryption on this data is very weak, it is a simple XOR based encryption, with a fixed 256 byte mask. In order to change the configuration, this key must be known. Once this key is known and the new configuration data is encrypted with it, and the new data can simply be posted to the httpd, the new configuration will take effect.

Successful exploitation of this vulnerability would allow an unauthenticated user the ability to modify the configuration of the affected router, including the password. This could allow firewall rules to be changed, installation of a new firmware with other features, or denial of service. Exploitation of this vulnerability would require that

an attacker can connect to the web management port of the router. The HTTPd is running by default but is only accessible via the LAN ports or the WLAN (wireless LAN).

An attacker who can associate with a network running a vulnerable HTTPd could send an exploit from a wireless device to reset the password on the device and enable the remote management port, allowing continued internet access.

Authentication credentials may be set if another user has attempted to view a page since the router was restarted. An attacker may be able to crash the HTTPd using another vulnerability, in which case it will restart within 2 minutes, with no authentication details initialized.

This would then allow them to exploit the HTTPd with this vulnerability.

#### Workaround:

In order to prevent exposure of this vulnerability from wireless clients, disable wireless access to the web interface:

- \* Connect to the web interface, typically at <http://192.168.1.1/>
- \* Go to the Administration page
- \* Select 'Disable' next to the 'Wireless Access Web'
- \* Click the 'Save Settings' button.

Please note that this will only prevent wireless access, and not access from one of the physical ports. Additionally, other vulnerabilities in the HTTPd may allow exploitation of the router, even with this setting enabled.

#### Dos:

The vulnerability exists in several of the "POST" method handlers of the HTTPd running on the router's internal interfaces, including by default the wireless interface. In addition to not checking if authentication has failed until after data supplied by an external user has been processed, there are several places where the Content-Length is assumed to be valid. In some of those cases, data is read in without error checking while decrementing the length value. If the Content Length is set to a negative number, these checks will take an extremely long time, during which the HTTPd will become unresponsive.

An unauthenticated remote attacker may cause a DoS on the affected router. Exploitation of this vulnerability would require that an attacker can connect to the web management port of the router. The HTTPd is running by default, but is only accessible via the LAN ports or the WLAN (wireless LAN).

Although this DoS is against the HTTPd itself, it may cause a higher than normal load on the router, which may be sufficient to cause packet loss. The HTTPd will also be unavailable. This may be sufficient to cause to owner to restart the device, which could in turn trigger changes made by a previous vulnerability.

Securiteam: [NEWS] Linksys WRT54G Router Multiple Vulnerabilities (Buffer Overflow, Multiple Authentication Bypass,

Remote exploitation of an input validation error within the web management HTTPd component of Linksys WRT54G wireless router may allow unauthenticated users to cause a denial of service (DoS).

Vendor Status:

This vulnerability is addressed in firmware version 4.20.7 available for download at:

<[http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL\\_Download\\_C2%26ci](http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL_Download_C2%26ci)  
WRT54G – Wireless–G Broadband Router V4.0

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2799>>  
CAN-2005-2799

06/07/2005 Initial vendor notification – Buffer overflow, Authentication Bypass – Initial vendor response – Buffer overflow, Authentication Bypass  
07/05/2005 Initial vendor notification – Authentication Bypass, DoS  
07/25/2005 Initial vendor response – Authentication Bypass, DoS  
09/13/2005 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@lists.iddefense.com>> iDEFENSE Labs Security Advisories.

The original article can be found at:

<<http://www.iddefense.com/application/poi/display?id=304&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=304&type=vulnerabilities>,

<<http://www.iddefense.com/application/poi/display?id=305&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=305&type=vulnerabilities>,

<<http://www.iddefense.com/application/poi/display?id=306&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=306&type=vulnerabilities>,

<<http://www.iddefense.com/application/poi/display?id=307&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=307&type=vulnerabilities>,

<<http://www.iddefense.com/application/poi/display?id=308&type=vulnerabilities>>  
<http://www.iddefense.com/application/poi/display?id=308&type=vulnerabilities>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

Securiteam: [NEWS] Linksys WRT54G Router Multiple Vulnerabilities (Buffer Overflow, Multiple Authentication Bypass,

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.