

# [NEWS] Dell TrueMobile 2300 Wireless Broadband Router Authentication Bypass

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00017.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Dec 2005 16:08:41 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

## Dell TrueMobile 2300 Wireless Broadband Router Authentication Bypass

---

### SUMMARY

"The  
<<http://support.dell.com/support/edocs/network/p57205/en/intro/index.htm>>  
Dell TrueMobile 2300 Wireless Broadband Router is an 802.11b/g wireless access point with a built-in Internet router."

Lack of authentication checking allows attackers to reset the authentication credentials on Dell TrueMobile 2300 Wireless Broadband Router without needing to know the previously chosen credentials.

### DETAILS

#### Vulnerable Systems:

- \* Dell TrueMobile 2300 firmware version 3.0.0.8, dated 07/24/2003
- \* Dell TrueMobile 2300 firmware version 5.1.1.6, dated 1/31/2004
- \* Previous versions of the firmware may also be affected, however it is not clear in which version the vulnerability was introduced.

The Dell TrueMobile 2300 is a wireless router and access point. By requesting the following url from the router, it is possible to obtain a

## [NEWS] Dell TrueMobile 2300 Wireless Broadband Router Authentication Bypass

page containing a form which allows you to reset the authentication credentials. (The IP is typically 192.168.2.1, and [ROUTER IP] should be replace by the router's actual address.)

[http://\[ROUTER IP\]/apply.cgi?Page=adv\\_password.asp&action=ClearLog](http://[ROUTER IP]/apply.cgi?Page=adv_password.asp&action=ClearLog)

Although dialog boxes for entering the username and password appear, pressing cancel will not prevent this exploit from working.

Exploitation allow remote attackers to associate with the internal side of the router to change any configuration settings, including uploading of new firmware.

The precise cause of the error is unknown. Although there is GPL source code available for this product, the firmware's source code version has not been kept up to date with the binary version. As a result, it does not directly allow the cause of the vulnerability to be determined.

Based on analysis of the affected binary, /usr/sbin/httpd, and the previous version of the source code it appears the cause is a logic error involving the 'ClearLog' string being checked without first ascertaining that the page was one where that made sense. Although the binary appears to be largely the same code as the available source code, there are many differences. In the binary version, the authentication is not performed in the same order as in the source version. It is likely that the determination of which pages to check is now done on the basis of the 'action' variable, rather than the previous method of using the page name.

### Vendor Status:

"The vendor is no longer selling this product and has replaced it with newer models that do not exhibit the defect. Therefore, a patch will not be released to address this issue."

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3661>>  
CVE-2005-3661

### Disclosure Timeline:

11/17/2005 – Initial vendor notification  
11/18/2005 – Initial vendor response  
12/07/2005 – Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idelabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE.

The original article can be found at:

<<http://www.odefense.com/application/poi/display?id=348&type=vulnerabilities>>  
<http://www.odefense.com/application/poi/display?id=348&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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.

- 
- Prev by Date: [\*\*\[NT\] Total Commander WCX FTP.INI FTP Account Information Weak Encryption\*\*](#)
  - Next by Date: [\*\*\[EXPL\] Microsoft Windows CreateRemoteThread DoS \(Exploit\)\*\*](#)
  - Previous by thread: [\*\*\[NT\] Total Commander WCX FTP.INI FTP Account Information Weak Encryption\*\*](#)
  - Next by thread: [\*\*\[EXPL\] Microsoft Windows CreateRemoteThread DoS \(Exploit\)\*\*](#)
  - Index(es):
    - ◆ [\*\*Date\*\*](#)
    - ◆ [\*\*Thread\*\*](#)