

# [NEWS] UTStarcom F1000 VoIP Wifi Phone Multiple Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0070.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 11/21/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 21 Nov 2005 16:32:28 +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>

-----

UTStarcom F1000 VoIP Wifi Phone Multiple Vulnerabilities

---

## SUMMARY

<<http://www.utstar.com/Solutions/Handsets/WiFi/>> F1000 – "The residential Wi-Fi handset is a revolutionary device that expands the reach of VoIP communications. It provides consumers a new cost effective way to communicate, with great features such as 3-way Calling, Call Waiting, Call Transfer and many popular features."

Multiple security vulnerabilities have been discovered discovered in UTStartcom's Wifi VoIP solution.

## DETAILS

Vulnerable Systems:

- \* UTStarcom F1000 VOIP WIFI Phone
- \* Factory Firmware version 5.5.1. (Kernel: WIND version 2.6. Made on Apr 5 2005, 14:49:39)

Vendor Status:

Vendor notified on 27 June, 2005 via [sales@utstarcom.com](mailto:sales@utstarcom.com)

## Securiteam: [NEWS] UTStarcom F1000 VoIP Wifi Phone Multiple Vulnerabilities

UTStarcom F1000 VoIP Wifi phone SNMP daemon:

UTStarcom F1000 VoIP Wifi phone SNMP daemon has default public read credentials and the daemon cannot be disabled. UTstarcom F1000 SNMP daemon default public credentials allows an attacker with access to the phone's SNMP daemon to read the phone's SNMP configuration. This can lead to sensitive information disclosure. In addition, the daemon's read/write credentials cannot be changed, nor can the daemon be disabled via the phone's physical interface (i.e. via keypad input). During testing, the SNMP daemon appeared consistently die when connecting via Snmpwalk, requiring rebooting the phone in order to restore SNMP service.

UTstarcom F1000 VoIP Wifi Phone telnet server:

UTstarcom F1000 VoIP Wifi Phone telnet server has known default user/password credentials. The phone's operating system is Wind River's Vxworks. Default credentials for this OS are publically known to be target/password.

By default, the telnet daemon is listening on the phone (TCP port 23) providing WIFI network access to the phone's OS. Attackers can telnet to the phone and gain access to the phone's Vxworks OS using the known default credentials.

Impact is full access to the Vxworks OS, including debugging, direct memory dumping/injection, read/write device, user and network configuration files, enable/disable/restart services, remote reboot. For a workaround, the default login/password can be changed.

UTstarcom F1000 VoIP Wifi Phone rlogin (TCP/513) unauthenticated access:

The phone's rlogin port TCP/513 is listening by default and requires no authentication. An attacker connecting to the phone via telnet/netcat is dropped into a shell without any login. The shell provides an attacker full access to the Vxworks OS, including debugging, direct memory dumping/injection, read/write device, user and network configuration files, enable/disable/restart services, remote reboot.

There appears to be no workaround as neither the service can be disabled, nor can authentication to rlogin be enabled.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:shawnmer@gmail.com> Shawn Merdinger.

=====

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

**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.