

# UTStarcom B-NAS 1000 / B-RAS 1000 Major Security Flaw

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-08/0345.html>

---

*From:* Scott T. Cameron ([karn@routehero.com](mailto:karn@routehero.com))

*Date:* 08/23/02

Date: Fri, 23 Aug 2002 12:26:40 -0700  
From: "Scott T. Cameron" <[karn@routehero.com](mailto:karn@routehero.com)>  
To: [bugtraq@securityfocus.org](mailto:bugtraq@securityfocus.org)

== Overview ==

UTStarcom [<http://www.ustar.com>] is a broadband DSLAM and DSL SMS hardware vendor. Their products are used to manage DSL through PPPoE, PPPoA, bridge mode etc.

== Vulnerability ==

The vendor (UTStarcom) has placed 2 backdoor accounts with full system access in their BAS-1000 system [B-RAS 1000]. (Formerly known as an Issanni 1000 [<http://www.issanni.com>]) One account is approximately equal to the account the customer will have, however, the customer can not see these users logged in, remove them, change access levels or change passwords.

It is a relatively simple process to find the usernames and passwords. Using the strings(1) command on the latest firmware revision, I was able to find this:

```
-- begin --  
Development engineer (this option is restricted)  
guru  
Field engineer (this option is restricted)  
field  
Management user with full system privileges  
manager  
Management user with limited write privileges  
administrator  
Management user with read-only privileges  
operator  
-- end --
```

This shows us that there are 2 access-levels beyond what the 'manager' accounts can see, both 'field' and 'guru'.

Going further through the strings, we find in plaintext the usernames and passwords:

```
-- begin --  
MANAGEMENT_USERS
```

## SecurityFocus Bugtraq: UTStarcom B-NAS 1000 / B-RAS 1000 Major Security Flaw

```
initializing module %s
initialized module %s
OPER
Failed to create permanent user "%s"
ADMIN
*field
FIELD
*3noguru
GURU
SNMP
DBASE
-- end --
```

We now know that the login name 'field' has a password of '\*field'. This account is approximately equal to the manager level accounts.

We also now know the login name 'guru' has a password of '\*3noguru'. This account has higher access to a few more system abilities that the customer would not ordinarily see.

When we log in with the 'guru' account, we can see a couple more users even:

```
-- begin --
                                     Active
Management User Name Access Level Logins Last Login Time
-----
mgr manager 0 08/22/02 09:48:18
oper operator 0 <Never>
admin admin 0 <Never>
field field 0 08/21/02 16:26:28
guru guru 1 08/22/02 09:48:28
snmp snmp 0 <Never>
dbase dbase 0 <Never>
-- end --
```

'snmp' and 'dbase' are not ordinarily login names that appear for the standard 'mgr' account. They have the password of their username. Which is to say:

account 'snmp' has a password of 'snmp'.

account 'dbase' has a password of 'dbase'.

Note, you can not ordinarily see these users via the mgr user.

== Impact ==

Any user with the IP of the management port will be able to log in with full system privileges.

== Workaround ==

Log in as the 'mgr' account and add in an ACL for your management port to deny access appropriately so only the correct individuals have access to the unit. Unfortunately,

## SecurityFocus Bugtraq: UTStarcom B-NAS 1000 / B-RAS 1000 Major Security Flaw

in version 3.1.10 of the firmware (the most recent), there is a bug which allows anyone to pass through ACLs.

One thing you can do is change the passwords of the accounts. Log in with the guru, field, snmp or dbase accounts, and issue the command:

```
conf manage <user> change-password <old password> <new password>
```

I highly recommend this to prevent anyone from logging in via these accounts and abusing your system.

== Vendor Reply ==

As far as the hidden accounts, yes, there are two accounts used by UTStarcom personel for debug purposes. The "field" account is used by field application engineers with some "engineering" type debugging information available. Currently, this user is identical to the "mgr" user. The "guru" account is used by development to get debug information and debug access to the system. It has some privledges that are not generally available.

As far as security. There are a couple of levels of security for the management port in increasing security order.

- 1) Username/Password only.
- 2) added management ACL
- 3) added firewall system in front of management port
- 4) remove management ethernet and add dial-in modem to serial port

Most of our customers have their management port on a secure network (either using a firewall or the management ACLs), so this is not much of an issue.

As far as changes, it is possible to encrypt the passwords in an upcoming release (as well as change the hidden account passwords) as to foil a strings command. We do not have this in our current development plan however.

== End Vendor Reply ==

Regards,  
Scott T. Cameron

---

- **Previous message:** [Rich Lafferty: "Re: \[luca.ercoli@inwind.it: DoS against mysqld\]"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)