

# Weakness introduced by denying remote logins on AIX, possibly others

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-02/0158.html>

---

**From:** Scott J ([mrbinary\\_at\\_yahoo.com](mailto:mrbinary_at_yahoo.com))

**Date:** 02/10/04

Date: 10 Feb 2004 13:10:50 -0000  
To: security-basics@securityfocus.com

('binary' encoding is not supported, stored as-is)

This advisory was submitted to BugTraq July 2003 – it was rejected as being a known issue / config problem type of thing. I am submitting it to this list as I believe that it is very likely that an individual or group new to the security field will at some point change the configuration of an AIX server to prevent direct login for some accounts (particularly root), and they may be unaware of all of the ramifications that taking this action results in.

Email exchanges with BugTraq personnel (in July of last year) were the source of info that indicated Solaris may suffer from the same issue.

Currently, BPR personnel can neither confirm or deny this behaviour exists in any OS other than AIX of versions mentioned below.

----- BinaryPowered Research advisory 2003-01 (revised)  
-----

This advisory may be reproduced and redistributed in any manner.  
BPR and the author(s) of this advisory assume no liability for any misuse of information contained in this advisory. Neither BPR nor the author(s) are in any way liable for any damages caused by or believed to arise from this advisory.

----- BinaryPowered Research advisory 2003-01  
-----

Abstract: Remote password enumeration possible for  
          accounts not permitted direct login in AIX  
Affected Systems: AIX 4.3.3 and AIX 5.1, likely other levels of AIX  
Vendor: International Business Machines Corporation (IBM)  
Severity: Low  
Result: Privilege escalation possible depending upon circumstances  
Vendor Notified: YES  
Vendor Response: Within one day  
Patch Issued: None available.  
Release date: 2003-07-17  
Rereleased: 2004-02-06

## SecurityFocus BASICS: Weakness introduced by denying remote logins on AIX, possibly others

### Discussion:

During some configuration change and testing of AIX for a client, BPR discovered that it is possible to remotely enumerate the passwords of a known AIX account. The only configuration change required to allow this to happen in AIX is to disable remote logins for a given account (via the command "chuser rlogin=false a\_userid"). If a remote attacker tries to connect to the vulnerable machine with an incorrect password (but a known correct account name), the response from AIX will be:

"3004-007 You entered an invalid login name or password."

In the case that the correct password is provided, the response is as follows:

"3004-306 Remote logins are not allowed for this account." This different, unique response allows an attacker to determine the password of the account in question.

### Known Vulnerable:

AIX 4.3.3 maintenance level 10 applied – assume all levels of AIX 4.3.3

AIX 5.1 maintenance level 4 applied – assume all levels of AIX 5.1

### Rumored Vulnerable:

Solaris (no version information available – not tested by BPR)

### Completely Untested / Unknown:

Linux

OpenBSD

NetBSD

FreeBSD

BSD/OS

HP-UX

IRIX

SCO

### Vulnerable authentication methods tested and verified:

Local

LDAP

### Access methods tested and verified:

telnet

rlogin

rsh

ssh ( OpenSSH – no commercial SSH variant tested )

++ Note: OpenSSH version most recently tested was the prepackaged version for AIX 5.1 currently available (as of Feb. 2004) on DeveloperWorks at:

<http://oss.software.ibm.com/developerworks/projects/opensshi>

It's not known for certain if this weakness would exist for an in-house compiled version of Portable OpenSSH on AIX but as the weakness is believed to be in the response from the login program after authentication

## SecurityFocus BASICS: Weakness introduced by denying remote logins on AIX, possibly others

has taken place, it would also likely be affected. Also, it makes no difference if sshd is configured to allow or disallow root login via the PermitRootLogin option.

### Exacerbating Factors:

AIX only stores the first 8 characters of the password – if those first 8 characters are correct, the login will succeed, despite the fact that AIX's login program will accept passwords longer than 8 characters. I believe that the login program only stores and encrypts the first 8 characters (this is speculation on my part, others on the list may know more definitively). This "weakness" also applies to the remote evaluation of a password of course, since the value stored for a password is only the encrypted equivalent of the first 8 characters.

### Mitigating Factors:

To "exploit" this the attacker would have to have the ability to log on to the host in question with another userid since the account whose password has been enumerated obviously cannot be used for remote login. Alternately the attacker would require local (ie tty-equivalent) access to the machine. Worth noting is the fact that as long as the password is complex and is 8 characters, it will take a significant amount of time to determine the password of a target userid, possibly thousands or hundreds of thousands of years to determine via brute-force using a remote connection.

### Severity:

In a relatively "safe" environment such as a small business where external network logins are blocked this can be considered low priority but in a more hostile environment such as a service provider that permits shell-level access and has a relatively untrustworthy userbase it should be considered much more dangerous if short or weak passwords are used for critical accounts.

### Solution:

The correct solution would be to change the messages so that the response is consistent whether a correct or incorrect password is supplied. In AIX the messages that are returned for the various login actions can be found in /usr/lib/nls/msg/\$LANG/tsm.cat and /usr/lib/nls/msg/\$LANG/libs.cat. To change them, perform the following:

```
dspscat -g /usr/lib/nls/msg/$LANG/libs.cat > /tmp/new_libs.msg
```

Change message in /tmp/new\_libs.msg to make the messages consistent with one another

Create the new catalog file, issue:

```
gencat CatalogFile SourceFile
```

Finally, copy message catalog back to it's intended location and test. This "customized" message catalog will quite possibly be wiped out by maintenance level upgrades etc. to AIX, so this would need to be verified and possibly repeated whenever an OS upgrade is performed, if it makes any changes to the relevant message catalogs.

Other suggestions to reduce exposure (but not eliminate it entirely):

Give accounts that have been restricted from remote logins strong passwords.

Change accounts that have been restricted from remote logins such that only specified

## SecurityFocus BASICS: Weakness introduced by denying remote logins on AIX, possibly others

groups can su to that account (similar to the "wheel" group concept in BSD).

Change the delay for unsuccessful login attempts (via the "logindelay" parm in the login.cfg file). For every second that you increase the logindelay value, you make a bruteforce attack less likely to succeed by a corresponding magnitude.

If your site is not already doing so ensure that unsuccessful login attempts are monitored with alerts sent to a human-monitored facility when unsuccessful login counts become too high.

Where practical, suspend / lock accounts automatically when unsuccessful login thresholds are exceeded.

Ensure that critical accounts have strong passwords, and have password strength enforcement in place.

Vendor Response (paraphrased):

=This is the expected response of AIX. This behaviour can be changed by performing the following.... (outlined above) To have this default behaviour changed, contact an IBM marketing rep to initiate a process called "Design Change Request".=

BPR Response:

It is disappointing that this is the out-of-the-box behaviour of an operating system that is a current offering of one of the largest computer hardware and software vendors in the market. Furthermore, it is quite bizarre to suggest that a customer should have to contact a marketing representative to request such a change in behaviour, technical people and security professionals at IBM should realize the need to change this behaviour, especially given how easy it would be to correct it.

Closing Remarks:

As the root account is the most powerful account on the system logic dictates that if a site is trying to improve the security posture of their AIX host(s), root accounts are among the most likely to be disabled for remote logins. This is generally a good measure to take, but particularly so when the password strength is effectively limited to 8 characters. Also, it is highly unusual to have the root account automatically suspended because of invalid login attempts as this would require rebooting the server and bringing it into single user mode to correct. Taking these factors into account, root becomes the most likely to have attempted enumeration of it's password performed via brute-force methods. Furthermore, it is rare that the account with UID=0 will have had the account name associated with it changed from root, it can introduce difficult-to-diagnose problems including but probably not limited to idiotic major software vendors whose software install scripts do not validate that it is UID 0 invoking the install scripts, but instead perform a whoami inquiry expecting "root" to be the returned value.

---

Free trial: Astaro Security Linux — firewall with Spam/Virus Protection

Protect your network with the comprehensive security solution that integrates six applications for ease of use and lower TCO.

SecurityFocus BASICS: Weakness introduced by denying remote logins on AIX, possibly others

Firewall – Virus protection – Spam protection – URL blocking – VPN  
– Wireless security.

Download 30-day evaluation at:

<http://www.astaro.com/php/contact/securityfocus.php>

---