AIX v3 Security Notice Regarding Root Access (9/94)

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

> **Note:** The information in this document has **not** been verified for AIX 4.1.

About this Document

This document is based on an AIX Service Bulletin dated September 8, 1994. It contains a procedure for eliminating an AIX version 3 unauthorized root security exposure.

Overview

IBM has become aware of a potential security exposure in all releases and levels of AIX Version 3 that could allow local and remote users to obtain unauthorized root authority. This unauthorized root authority may be obtained through the use of:

- The vi editor
- Remote login
- The batch (bsh) queue
- Network Information Service (NIS)

Officially released fixes, IX43595, IX44254, IX44381, and IX44685, can be obtained using FixDist, or from the IBM Support Center.

Customers can also chose to perform the procedures outlined on the attached pages to immediately eliminate the potential exposure, although this will disable the remote login, batch queue, and NIS functions.

Additionally, IBM has become aware of a potential problem affecting only AIX Version 3.2.5 that could allow a user program to abnormally terminate ("crash")

a system, requiring a system reboot. A fix for this problem, IX44274, can be obtained using FixDist in the U.S., or from the IBM Support Center.

For information on contacting the IBM Support Center, call 800-IBM-4FAX and request document number 1760.

Procedure

1. Log in as root.
2. To ensure that root's shell is /bin/ksh, use the following command:

   ```
   /bin/ksh
   ```

3. To ensure that your current directory is root (/), use the following command:

   ```
   cd /
   ```

   The following steps eliminate the ability to obtain unauthorized root access through the use of the vi editor. The vi editor may be used to accomplish these steps.

4. Determine the version of the vi editor using the following command:

   ```
   strings /usr/bin/vi | grep ex_data
   ```

   If the second column of output is '1.6' or '1.7', then perform steps 5 and 6, otherwise skip to step 7.

5. Create or edit the existing .exrc file in the home directory of every user, starting with root, and insert the following as the first line:

   ```
   set nosourceany noexrc
   ```

6. Set the owner and permissions of the .exrc file using the following command, substituting the user name for "<user>":

   ```
   chown <user>  <user>/.exrc
   chmod 600  <user>/.exrc
   ```

The following steps eliminate remote login (rlogin and rsh).

7. Edit the /etc/inetd.conf file. If the following line exists, comment it out by inserting a # in the first column of the line:

   ```
   login  stream  tcp  nowait  root  /etc/rlogind  rlogind
   ```

8. Enter the following commands to make the change take immediate effect:

   ```
   /usr/bin/inetimp
   /usr/bin/refresh -s inetd
   ```

   The following step eliminates the ability to obtain unauthorized root access through the use of the batch (bsh) queue.

9. Enter the following command to disable the batch queue:

   ```
   /usr/bin/chque -qbsh -a"up = FALSE"
   ```

The following steps eliminate the ability to obtain unauthorized root authority through the use of NIS by disabling NIS on the client.

10. Copy the /etc/hosts, /etc/passwd, /etc/security/passwd, /etc/group, /etc/security/group and any other NIS served files from the NIS master to the NIS client.
11. Enter the following command on the NIS client to disable NIS on the client:

```
/usr/etc/yp/rmyp -c
```

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

04/14/95

END OF DOCUMENT (security.letter.gen, 4FAX# 1826)