IBM SECURITY ADVISORY

First Issued: Thu Dec 8 15:00:32 CST 2005

VULNERABILITY SUMMARY

VULNERABILITY:	Insecure file permissions may allow a denial of service.
PLATFORMS:	IBM Director Server and Console 5.10 for AIX 5.3
SOLUTION:	Upgrade IBM Director or apply the workaround as described below.
THREAT:	A local user may cause a denial of service
CERT VU Number:	N/A
CVE Number:	N/A

DETAILED INFORMATION

I. Description

IBM Director Server and Console 5.10 (VRMF 5.10.0.0) modify the file mode bits and ownership of / and /opt when installed. The new file mode bits will allow any local user to write to / or /opt. An attacker may be able to cause a denial of service or carry out other malicious activity.

The file permissions are changed when any of the following filesets are installed:

IBM.Director.Server.common.SeriesLib.rte
IBM.Director.Server.ext.BladeCenter.rte
IBM.Director.Server.ext.xSeries.rte
IBM.Director.Server.ext.RackManager.rte
IBM.Director.Console.common.SeriesLib.rte
IBM.Director.Console.ext.BladeCenter.rte
IBM.Director.Console.ext.xSeries.rte
IBM.Director.Console.ext.RackManager.rte

To determine if any of these filesets are installed, execute the following command:

```
# lslpp -L <fileset name>
```

If the fileset is installed it will be listed along with its version information, state, type and a description. The vulnerable versions of these filesets have a version number of 5.10.0.0

II. Impact

A local user may cause a denial of service or carry out other malicious activity.

III. Solutions

A. Official Fix

IBM provides an IBM Director 5.10 refresh for AIX to address this issue. The refreshed IBM Director 5.10 for AIX package can be downloaded from:

https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=dmp

or

http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-61777

The affected filesets have been upgraded to 5.10.0.1. Installing the updated filesets will restore the file mode bits and ownership for / and /opt.

B. Workaround

Restore the file mode bits

Restoring the file mode bits and ownership for / and /opt will remove this vulnerability. To restore the file mode bits, execute the following commands as the root user:

```
# chown root:system /
# chmod 755 /
# chown root:system /opt
# chown 755 /opt
```

Verify that the file mode bits have been updated:

```
# ls -ld / /opt
# drwxr-xr-x  26 root     system         4096 Dec 04 06:07 //
# drwxr-xr-x   9 root     system          256 Jul 08 14:06 /opt/
```

Note: Some versions of AIX may not display the trailing '/'

IV. Obtaining Fixes

AIX Version 5 APARs can be downloaded from:

http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html

IBM Director and be downloaded from:

https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=dmp

or

http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-61777

V. Contact Information

If you would like to receive AIX Security Advisories via email, please visit:

https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs

Comments regarding the content of this announcement can be directed to:

security-alert@austin.ibm.com

To request the PGP public key that can be used to communicate securely with the AIX Security Team send email to security-alert@austin.ibm.com with a subject of "get key". The key can also be downloaded from a PGP Public Key Server. The key id is 0x9391C1F2.

Please contact your local IBM AIX support center for any assistance.