

Re: [VulnWatch] iDEFENSE Security Advisory 02.08.05: IBM AIX auditselect Local Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-02/0008.html>

From: Shiva Persaud (*shivapd_at_us.ibm.com*)

Date: 02/09/05

To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

Date: Tue, 8 Feb 2005 17:43:14 -0700

The IBM advisory for this issue:

<BEGIN>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

IBM SECURITY ADVISORY

First Issued: Tue Feb 8 18:07:01 CST 2005

=====

VULNERABILITY SUMMARY

VULNERABILITY: A format string vulnerability in the auditselect command may allow a local user in the audit group to gain root privileges.

PLATFORMS: AIX 5.1, 5.2 and 5.3.

SOLUTION: Apply the workaround or APARs as described below.

THREAT: A local user may gain root privileges.

CERT VU Number: N/A

CVE Number: N/A

=====

DETAILED INFORMATION

I. Description

=====

A format string vulnerability in the auditselect command was discovered. This vulnerability may allow a local user in the audit group to gain root

privileges.

The command affected by this issue ships as part of the bos.rte.security fileset. To determine if this fileset is installed, execute the following command:

```
# lspp -L bos.rte.security
```

If the fileset is installed it will be listed along with its version information, state, type and a description.

II. Impact

=====

A local user in the audit group may gain root privileges.

III. Solutions

=====

A. Official Fix

IBM provides the following fixes:

APAR number for AIX 5.1.0: IY67802 (available approx. 03/23/05)

APAR number for AIX 5.2.0: IY67472 (available approx. 04/15/05)

APAR number for AIX 5.3.0: IY67519 (available approx. 04/15/05)

NOTE: Affected customers are urged to upgrade to 5.1.0, 5.2.0 or 5.3.0 at the latest maintenance level.

B. Workaround

Setting the file mode bits to 500 will allow only the root user to execute the auditselect command. This can be done by executing the following command as root:

```
# chmod 500 /usr/sbin/auditselect
```

Verify that the file mode bits have been changed to 500:

```
# ls -la /usr/sbin/auditselect
```

```
--r-x----- 1 root audit 20778 2002-09-15 22:09 /usr/sbin/auditselect
```

IV. Obtaining Fixes

=====

AIX Version 5 APARs can be downloaded from:

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

Security related Emergency Fixes can be downloaded from:

<ftp://aix.software.ibm.com/aix/efixes/security>

V. Acknowledgments

=====

This vulnerability was reported by iDEFENSE.

VI. Contact Information

=====

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

<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc>

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.

eServer is a trademark of International Business Machines Corporation. IBM, AIX and pSeries are registered trademarks of International Business Machines Corporation. All other trademarks are property of their respective holders.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.0 (MingW32)

iD8DBQFCCVb5xwSSvpORwfIRAvnXAJ9sxokSMPEj9JRzSF0hPWYeO0f0QgCcCJUB
PaTHBDsOAP5kx4Z7UienWU8=
=hsTE

-----END PGP SIGNATURE-----

</BEGIN>

-
- application/x-pkcs7-signature attachment: [S/MIME Cryptographic Signature](#)