

# [UNIX] Buffer Overflow in AIX libIM.a

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0027.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 02/13/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Feb 2003 17:49:25 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Buffer Overflow in AIX libIM.a

---

## SUMMARY

Advanced Interactive eXecutive (AIX) is IBM Corp.'s UNIX operating system implementation, native to pSeries and RS/6000 servers. More information is available at <http://www-1.ibm.com/servers/aix/> <http://www-1.ibm.com/servers/aix/>.

AIX provides support for National Language Support (NLS). From the AIX manual available at

[http://publib16.boulder.ibm.com/doc link/en\\_US/a doc lib/aixprgdd/nlsgrdf/nat lang support.htm](http://publib16.boulder.ibm.com/doc link/en_US/a doc lib/aixprgdd/nlsgrdf/nat lang support.htm),> [http://publib16.boulder.ibm.com/doc link/en\\_US/a doc lib/aixprgdd/nlsgrdf/nat lang support.htm](http://publib16.boulder.ibm.com/doc link/en_US/a doc lib/aixprgdd/nlsgrdf/nat lang support.htm), "NLS

provides commands and Standard C Library subroutines for a single worldwide system base. An internationalized system has no built-in assumptions or dependencies on language-specific or cultural-specific conventions such as:

- \* Code sets
- \* Character classifications
- \* Character comparison rules
- \* Character collation order
- \* Numeric and monetary formatting
- \* Date and time formatting
- \* Message-text language

All information pertaining to cultural conventions and language is



## Securiteam: [UNIX] Buffer Overflow in AIX libIM.a

Illegal instruction (reserved addressing fault) in . at 0x11223344 (\$t1)  
warning: Unable to access address 0x11223344 from core 0x11223344 (???)  
warning: Unable to access address  
0x11223344 from core ffffffff warning: Unable to access address  
0x11223344 from core fnmadd.  
fr31,fr31,fr31,fr31 (dbx)

Vendor response:

A. E-fix

Temporary fixes for AIX 4.3.3, 5.1.0, and 5.2.0 systems are available.

The temporary fixes can be downloaded via ftp from:

<[ftp://aix.software.ibm.com/aix/efixes/security/libIM\\_efix.tar.Z](ftp://aix.software.ibm.com/aix/efixes/security/libIM_efix.tar.Z)>

[ftp://aix.software.ibm.com/aix/efixes/security/libIM\\_efix.tar.Z](ftp://aix.software.ibm.com/aix/efixes/security/libIM_efix.tar.Z)

The efix-compressed tarball contains three fixes: one each for AIX 4.3.3, AIX 5.1.0, and AIX 5.2.0. It also includes an advisory and a README file with installation instructions.

B. Official Fix

IBM will provide the following fixes:

- \* APAR number for AIX 4.3.3: IY40307
- \* APAR number for AIX 5.1.0: IY40317
- \* APAR number for AIX 5.2.0: IY40320

NOTE: Fixes will not be provided for versions prior to 4.3, as these are no longer supported by IBM. Affected customers are urged to upgrade to 4.3.3 or 5.1.0 at the latest maintenance level.

Disclosure timeline:

10/31/2002 Issue disclosed to iDEFENSE

01/28/2003 IBM notified ([security-alert@austin.ibm.com](mailto:security-alert@austin.ibm.com))

01/29/2003 Response received from Shiva Persaud ([shivapd@us.ibm.com](mailto:shivapd@us.ibm.com))

02/11/2003 iDEFENSE clients notified

02/12/2003 Coordinated Public Disclosure

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:labs@idefense.com>> iDEFENSE Labs, the vulnerability was discovered by <[mailto:ewan\\_briggs@btinternet.com](mailto:ewan_briggs@btinternet.com)> Euan Briggs.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

Securiteam: [UNIX] Buffer Overflow in AIX libIM.a

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.