

[UNIX] IBM AIX chdev Local Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/17/05

To: list@securiteam.com

Date: 17 Feb 2005 19:29:27 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

IBM AIX chdev Local Format String Vulnerability

SUMMARY

The chdev program is "a setuid root application, installed by default under multiple versions of IBM AIX, that facilitates the changing of device characteristics". Local exploitation of a format string vulnerability in the chdev command included by default in multiple versions of IBM Corp.'s AIX operating system could allow for arbitrary code execution as the root user.

DETAILS

Vulnerable Systems:

- * IBM AIX version 5.2

The vulnerability specifically exists due to an improperly used formatted printing function. When provided with an incorrect argument (`argv[1]`) that contains a format string, the format string will be fed into a formatted printing function, and the user supplied format string will be evaluated, allowing for a malicious user to examine stack memory and write to arbitrary memory locations. With a properly crafted string, this can lead to the execution of arbitrary code.

Securiteam: [UNIX] IBM AIX chdev Local Format String Vulnerability

Analysis:

This vulnerability can only be exploited by a local user who has been granted access to the "system" group. Successful exploitation leads to root-level access.

Due to the nature of the vulnerability, information leakage is trivial and aids the attacker in exploitation.

Workaround:

Only allow trusted users local access to security critical systems. Only allow trusted system administrators access to the "system" group. Alternately, remove the setuid bit from chdev using `chmod u-s /usr/sbin/chdev`.

Vendor response:

The vendor has not released a patch for this issue, however, the following details have been published:

<http://www-1.ibm.com/support/docview.wss?uid=isg1IY67455>
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY67455>

In addition, a security advisory will be posted at the following site:

<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc?mode=1>
<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc?mode=1>

Please note that a free signup is required to access the security advisory.

Disclosure Timeline:

12/21/2004 – Initial vendor notification
01/07/2005 – Initial vendor response
02/07/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:customerservice@idefense.com>> iDEFENSE.

The original article can be found at:
<<http://www.idefense.com/application/poi/display?type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?type=vulnerabilities>

=====

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

Securiteam: [UNIX] IBM AIX chdev Local Format String Vulnerability

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.