

[UNIX] IBM AIX ipl_varyon Local Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 13:31:06 +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 ipl_varyon Local Buffer Overflow Vulnerability

SUMMARY

The ipl_varyon program is "a setuid root application, installed by default under multiple versions of IBM AIX, which can be used to set the default physical boot volume".

Local exploitation of a buffer overflow vulnerability in the ipl_varyon 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 unbounded string copy operation. When provided with a long argument to the -d option, the ipl_varyon process will overwrite stack memory with the user supplied string. This allows for overwriting of the saved return address on the stack, which in turn allows for complete control over execution flow.

Securiteam: [UNIX] IBM AIX ipl_varyon Local Buffer Overflow Vulnerability

Analysis:

Exploitation of this vulnerability is simple for a skilled attacker, however gid "system" is required in order to execute the vulnerable binary. Successful exploitation yields root access on the system.

Workaround:

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

Vendor Status:

Vendor advisories for this issue are available at:

* For AIX 5.1:

<<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc?mode=1&heading=AIX51&topic=SECURITY&id=196>>
AIX 5.1 Security Advisories

* For AIX 5.2:

<<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc?mode=1&heading=AIX52&topic=SECURITY&id=196>>
AIX 5.2 Security Advisories

* For AIX 5.3:

<<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc?mode=1&heading=AIX53&topic=SECURITY&id=196>>
AIX 5.3 Security Advisories

Disclosure Timeline:

12/21/2004 – Initial vendor notification
01/07/2004 – Initial vendor response
02/10/2004 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=196&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=196&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 ipL_varyon Local Buffer Overflow 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.