

[UNIX] IBM AIX libodm ODMPATH Stack Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-07/msg00021.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 11 Jul 2007 10:21:17 +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 libodm ODMPATH Stack Overflow Vulnerability

SUMMARY

AIX applications "use libodm to access system settings and device configuration data stored in the Object Database Manager. The Manager is responsible for accessing and updating such things as currently installed software packages and devices. Many of the applications that use libodm are installed set-uid root". Local exploitation of a buffer overflow vulnerability in IBM Corp.'s AIX libodm library could allow an attacker to execute arbitrary code on a targeted host.

DETAILS

Vulnerable Systems:

- * AIX version 5.3 SP 4

The vulnerability exists in the processing of the ODMPATH environment variable within the odm_searchpath() function. This function reads the ODMPATH variable from the user provided environment, and then copies it into a fixed sized stack buffer without properly validating its length. This results in a stack-based buffer overflow, and allows the saved return address to be overwritten.

[UNIX] IBM AIX libodm ODMPATH Stack Overflow Vulnerability

Analysis:

Exploitation allows an attacker to execute code with root privileges.

Since this is a local attack, an attacker has complete control over the process environment and can reliably place shellcode at known addresses. This makes exploitation of this vulnerability trivial.

Vendor response:

IBM Corp. has addressed this vulnerability with interim fixes. More information is available at the following URL:

<<http://www-1.ibm.com/support/docview.wss?uid=isg1IY97632>>

<http://www-1.ibm.com/support/docview.wss?uid=isg1IY97632>

Disclosure timeline:

04/02/2007 – Initial vendor notification

04/05/2007 – Initial vendor response

07/09/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=552>>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=552>

=====

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@xxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

=====

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.