

[REVS] AIX Introduction to Heap Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 3 Jan 2006 10:08:28 +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>

AIX Introduction to Heap Overflows

SUMMARY

In the research paper linked here, David Litchfield explains how the heap works in the AIX operating system, and how to exploit heap based buffer overflows.

DETAILS

Exploiting heap overflows:

In terms of exploitation, one way to exploit heap overflows is with the "arbitrary 4 byte overwrite". When the pointers that keep track of heap blocks are updated, an attacker can influence this if they manage to overwrite the inline heap management data. On AIX, when an overflow occurs, to be able to gain control using the 4 byte overwrite one must overflow into the address pointed to by the next free block pointer at `__heaps+2580` or a block on the heap that points to a previously freed block.

When the pointer update occurs if we overwrite the real pointer with `0x12345678` then `0x12345678` is written to the address found at `0x12345680` (which is `0x12345678+8`.) So assuming at address `0x12345680` we have `0x11223344`, `0x12345678` is written to `0x11223344`. Further, the value stored

[REVS] AIX Introduction to Heap Overflows

at 0x12345684 is written to 0x11223348; on the other side, the value at 0x11223344 is written to 0x12345680 and the value at 0x11223348 is written to 0x12345684.

The full whitepaper can be found at:

<<http://www.databassecurity.com/dbsec/aix-heap.pdf>>
<http://www.databassecurity.com/dbsec/aix-heap.pdf>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:davidl@xxxxxxxxxxxxxxxx>>
David Litchfield.

The original article can be found at:

<<http://www.databassecurity.com/dbsec/aix-heap.pdf>>
<http://www.databassecurity.com/dbsec/aix-heap.pdf>

=====

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@xxxxxxxxxxxxxxxx

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

=====

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.

-
- Prev by Date: [***\[UNIX\] IceWarp Web Mail Multiple File Inclusion Vulnerabilities***](#)
 - Next by Date: [***\[EXPL\] aMSN Messenger DoS \(Send File\)***](#)
 - Previous by thread: [***\[UNIX\] IceWarp Web Mail Multiple File Inclusion Vulnerabilities***](#)
 - Next by thread: [***\[EXPL\] aMSN Messenger DoS \(Send File\)***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)