

[NT] Buffer Overflow in AOL Instant Messenger's Getfile Parameter

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0071.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/16/03

To: list@securiteam.com

Date: 16 Oct 2003 14:22:47 +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>

Buffer Overflow in AOL Instant Messenger's Getfile Parameter

SUMMARY

When AOL Instant Messenger (AIM) is installed, it installs the "aim" protocol handler. This protocol allows AIM to be loaded by arbitrary web pages by including an "aim:operation?parameter". One of these operations is getfile. This operation can be used to overflow an internal buffer, this can be used to overwrite the EIP address and execute arbitrary code.

DETAILS

Vulnerable systems:

- * AIM version 5.2.3292

Immune systems:

- * AIM version 5.5.3415 Beta

The operation getfile takes a parameter named "screenname". The getfile operation is used to retrieve a file from another user. When the operation is invoked, the user is warned about retrieving files. If the user clicks "OK" the file is normally sent to the requesting user. The warning dialog can be disabled by choosing "Don't ask me again!".

Securiteam: [NT] Buffer Overflow in AOL Instant Messenger's Getfile Parameter

A buffer overflow exists in the "screenname" parameter. The overflow allows an attacker to take control of EIP. The overflow allows arbitrary execution on the victim's machine.

The "aim" protocol has a strange security model. Many of the operations require no user interaction. One of the operations allows a web page to mark the user viewing the page as away and specify the text of the away message.

This behavior allows us to exploit the buffer overflow by setting the away text to be something like "I'm on vacation. Visit <http://server/vactionpics.html> to see my vacation pics". When the victim visits the web site, he or she is redirected to a URL with a maliciously crafted aim getfile protocol. The victim is then presented with the option of downloading the file. The victim will likely accept the warning since he or she is expecting to download some pictures from someone he or she trusts. Upon accepting the warning, the victim's machine is compromised.

Proof of Concept:

A link like `aim:getfile?screenname=[About 1130 chars]` will overwrite EIP. This bug is exploitable through a web page.

Resolution:

AOL has fixed this issue in AIM 5.5.3415 Beta. This update is available on http://www.aim.com/get_aim/win/win_beta.adp. Please note, AOL has not fixed the current non-beta version.

ADDITIONAL INFORMATION

The original advisory is available from:

<http://www.digitalpranksters.com/advisories/aol/AIMProtocolBO.html>
<http://www.digitalpranksters.com/advisories/aol/AIMProtocolBO.html>.

The information has been provided by ">AngryB .

=====

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`

=====

=====

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.