

Buffer Overflow in AOL Instant Messenger

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

From: DigitalPranksters (*secteam_at_DIGITALPRANKSTERS.COM*)

Date: 10/15/03

Date: Wed, 15 Oct 2003 03:34:33 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

DigitalPranksters Security Advisory

<http://www.DigitalPranksters.com>

AIM POP POP – Buffer Overflow in AOL Instant Messenger's screenname parameter of getfile

Risk: Medium

Product: AIM 5.2.3292 for Windows (Maybe others we only tested the latest version)

Product URL: <http://www.aim.com>

Vendor Contacted: September 16, 2003

Vendor Released Patch: September 25, 2003

DigitalPranksters Public Advisory Released: October 15, 2003

Found By: AngryB – angryb@digitalpranksters.com

Exploited By: AngryB – angryb@digitalpranksters.com
KrazySnake – krazysnake@digitalpranksters.com

Problem:

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 the operations is named "getfile". This operation 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!".

A buffer overflow exists in the "screenname" parameter. The overflow

NT-Bugtraq: Buffer Overflow in AOL Instant Messenger

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 further 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. We have internally created an exploit.

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.

Greetings:

SkippyInside, HTMLBCat, Spyder, Harmo, Purple Rain Man, and all people who responsibly disclose security bugs. It is you who help us learn while responsibly making systems more secure.

Thanks to AOL for fixing this issue.

Disclaimer:

Standard disclaimer applies. The opinions expressed in this advisory are our own and not of any company. The information within this advisory may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

NTBugtraq subscribers save \$103.00 off the TICSA exam by using promo code "NT1003" when registering to take the TICSA exam at www.2test.com. Prove to your employer and peers that you have the knowledge and abilities to be an active stakeholder in today's enterprise security. Become TICSA certified www.trusecure.com/ticsa. Promotion expires 12/31/03 and cannot be used in combination with other offers.
