

[NT] AOL Instant Messenger Remote Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0010.html>

From: support@securiteam.com

Date: 01/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 4 Jan 2002 00:37:32 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

AOL Instant Messenger Remote Buffer Overflow

SUMMARY

Internet Security Systems (ISS) X-Force has reported about a remote buffer overflow vulnerability in the popular AOL Instant Messenger (AIM) software. An exploit for this vulnerability has been released publicly.

This vulnerability may allow remote attackers to execute arbitrary commands on a victim's system. The victim is unable to refuse the request or determine who initiated the attack.

DETAILS

Affected versions:

AOL Instant Messenger versions 4.3 through 4.7.2480 for Windows

AOL Instant Messenger version 4.8.2616 for Windows (beta)

Note: AOL Instant Messenger versions prior to 4.3 have not been tested. Previous versions that contain the Games feature may also be vulnerable.

The AOL Instant Messenger program is used by over 100 million users to send messages, share, and transfer files, talk over the Internet, check stock prices and headlines, and play games.

Securiteam: [NT] AOL Instant Messenger Remote Buffer Overflow

A vulnerability exists in the code that processes game requests, which may allow attackers to execute arbitrary code on a remote AIM user's system. The victim is not able to refuse the game request in order to block the exploit. This vulnerability is relatively easy to exploit, and the exploit can contain a large and complex payload.

This is a serious vulnerability in a very widely used software product. If a worm like Code Red or Nimda were written to exploit this vulnerability, it would likely spread very rapidly, and could potentially damage both personal and business systems.

Recommendations:

ISS X-Force recommends that users upgrade to the latest version of AOL Instant Messenger as soon as a fix becomes available.

Until a fixed version of AOL Instant Messenger is available, system administrators are encouraged to block "login.oscar.aol.com" and port 5190 at the firewall. This will prevent AIM users from logging in to the AIM service.

To reduce the risk from this vulnerability until a fixed version is available, AOL Instant Messenger users should block unknown users from contacting them using AIM. However, this will not provide complete protection, because users on your Buddy List can still contact you. If this vulnerability is built into a worm, this attack may come from users on your Buddy List without their knowledge.

To block unknown users in AIM:

1. Go to My AIM -> Edit Options -> Edit Preferences.
2. In the left pane, select the Privacy category.
3. In the "Who can contact me" section, select "Allow only users on my Buddy List".

ADDITIONAL INFORMATION

The information has been provided by <mailto:xforce@iss.net> X-Force.

=====

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.

- *Previous message:* support@securiteam.com: "[NT] Security Risk When Using the CGI Binary (PHP.EXE) Under Apache"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)