

[NT] AOL AIM and ICQ File Transfer Path-Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 17 Apr 2007 19:19:21 +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>

AOL AIM and ICQ File Transfer Path-Traversal

SUMMARY

<<http://www.aim.com/>> AOL Instant Messenger and <<http://www.icq.com/>> ICQ are instant messaging applications that allow users to exchange messages and files.

Remote exploitation of a path-traversal vulnerability in AOL's AIM and ICQ could allow a remote attacker to place arbitrary files on the victim's machine during a file transfer operation.

DETAILS

Vulnerable Systems:

- * ICQ version 5.1.
- * AOL reported that AIM version 5.9 and prior are vulnerable.
- * (Previous versions are suspected vulnerable.)

AIM and ICQ allow users to share and transfer files via a custom protocol. During file transfers, the sender is allowed to specify the display name of the file, and the filename used for the transfer.

[NT] AOL AIM and ICQ File Transfer Path–Traversal

The recipient can only specify the folder in which to save the file. Due to an input validation flaw, the clients do not properly strip "../" traversal characters from the filename the attacker supplies. By specially encoding the path attackers can force the file to be saved to a directory of their choosing when the victim accepts the file transfer.

Exploitation of this vulnerability allows attackers to place arbitrarily named files in a directory of their choice when the victim accepts a file transfer.

By default ICQ warns users that file transfers are unsafe and to only accept file transfers from trusted users. ICQ also requires that a user is on your contact list in order to accept a file transfer. Users must manually accept the file transfer in order to be exploited.

During the file download, the traversal path is displayed in the filename portion of the dialog. ICQ will not overwrite existing files without prompting the user for confirmation. It is important to note that the attacker specifies the display name used in the file accept dialog. This file name is arbitrary and need not be the same as the actual file being transferred.

Vendor Status:

AOL has provided the following solutions to address this vulnerability.

1. Active ICQ clients have already been patched via an automatic update.
2. Users of the AIM client 5.9 and earlier are urged to upgrade to the latest version of the AIM client from <http://www.aim.com/>
3. In addition, AIM 5.9 users are also protected by a fix that has been applied to the AIM infrastructure."

Disclosure Timeline:

- * 02/01/2007 – Initial vendor notification
- * 02/01/2007 – Initial vendor response
- * 04/09/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=508>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=508>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[NT] AOL AIM and ICQ File Transfer Path-Traversal

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.