TheBillyGoatCurse.com

AOL Instant Messenger Browser Handling Vulnerabilities

Release date: August 9th, 2004

Date Discovered: July 20th, 2004

Severity: Highly Critical

Vendor: America Online

Vulnerable Software: AIM 5.5.3595 for Windows

Overview:

AOL Instant Messenger (AIM) utilizes browser handlers to allow for shortcuts in the form of URLs (ie I am away).

The aim:goaway handler is also able to execute a buffer overflow attack under certain circumstances. Internet Explorer prevents this attack by properly checking the length of the content that the handler passes the browser. On the other hand, a lengthy away message defined by aim:goaway will crash AIM in Mozilla-based browsers. It is suspected that the JavaScript parsing engine is the culprit in this case, as experiments seem to show that the IE JavaScript parser will not pass along lengthy variables while the Mozilla-based interpreter does.

Solution:
Use another client.

Vendor Solution:
A patch/upgrade is necessary to provide validation of both browser handling and memory management.

Vendor Status:
AOL has been notified but TheBillyGoatCurse.com has not been responded to yet.

Credits:
Ryan McGeehan - Ryan at TheBillyGoatCurse dot com
Kevin Benes - kgbenes at purdue dot edu
Greetz to pd

Copyright (c) 2004 TheBillyGoatCurse.com
Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express consent of **TheBillyGoatCurse.com**. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please email Ryan@TheBillyGoatCurse.com for permission.

Disclaimer
The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties, implied or express, with regard to this information. In no event shall the author be liable for any direct or indirect 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.