

FOR IMMEDIATE RELEASE

Press Contacts:

Martha Sherman
LogicLibrary, Inc.
412-471-4710
pr@logiclibrary.com

John Moran
Schwartz Communications, Inc.
781-684-0770
logiclibrary@schwartz-pr.com

LOGICLIBRARY UNCOVERS VULNERABILITY IN TRILLIAN INSTANT MESSAGING PRODUCT

Buffer Iteration Overflow Could Make Systems Susceptible to Attack

PITTSBURGH—March 23, 2005—LogicLibrary®, the leading provider of software development asset management tools, today announced it has uncovered a potential security vulnerability in the Trillian instant messaging client, produced by Cerulean Studios. The consequences of this vulnerability could range from an inconvenient program shut-down to a malicious hacker being able to gain control of a computer's operating system.

Trillian is a popular all-in-one instant messaging client used by over a million people on Windows operating systems. Supporting AIM, ICQ, MSN, Yahoo Messenger and IRC, Trillian allows users to be on several instant message and chat networks at the same time, using just a single client. Its extensible plug-in system, for services such as AIM, Yahoo, MSN and RSS, connects to an external Web server at various points. LogicLibrary's BugScan, an automated application security analysis solution, discovered a buffer iteration overflow in Trillian's handling of HTTP 1.1 response headers in several of these plug-in components.

The vulnerability originally appeared in Trillian 2.0. It was compounded because the same vulnerable code was included in several different components and locations. Although many instances of the bug were addressed in Trillian 3.0, at least two vulnerabilities persisted in the Yahoo IM component. These exploitable unbounded buffer iteration problems remain in the current product version, Trillian 3.1. There are at least two exploitable yahoo.dll buffer iteration bugs—one is at 0x520296c6 and the other is at 0x5201a05f.

Buffer overflows can result in arbitrary malicious code being executed on a vulnerable computer. An attacker can potentially gain control over the system being attacked, putting items such as private documents, sensitive financial information and e-mails at risk. BugScan has contacted Cerulean Studios about these issues on a number of occasions over the past 18 months, with the most recent correspondence taking place on February 23, 2005.

"In order to build trust and confidence in the quality of today's software, LogicLibrary believes it's crucial that vendors work closely together to fix problems and provide the public with as much information as possible," said Ralph Massaro, general manager, content products, LogicLibrary. "BugScan's ability to find the precise location of real, exploitable software bugs without needing access to source code can make an important contribution toward identifying and resolving possible problems before they cause harm."

It is recommended that Trillian users update their version to the latest 3.1 release and avoid using the Yahoo IM component until Trillian issues a patch.

As an adopter of the Organization for Internet Safety's (OIS) Guidelines for Security Vulnerability Reporting and Response, LogicLibrary summarized its findings in a Vulnerability Summary Report (VSR). This document was sent to Cerulean Studios for their consideration and action. The VSR can be viewed at: http://www.logiclibrary.com/trillian_vsr.pdf.

About LogicLibrary

LogicLibrary is the leading provider of software and services that make it possible for enterprises to manage and reuse software development assets (SDAs). The company's patent-pending technology provides a comprehensive and collaborative approach for creating, migrating and integrating enterprise applications for use in service-oriented architecture, Web services and other software development initiatives. Additionally, LogicLibrary's BugScan provides powerful, easy-to-use code-scanning technology that helps architects, developers and IT professionals ensure the highest levels of security throughout the software development lifecycle.

LogicLibrary has been positioned in the "Leader" quadrant in Gartner Inc.'s Magic Quadrant for Metadata Repositories, 2004* and maintains strategic partnerships with Microsoft, as a Premier member of the Visual Studio Industry Partner (VSIP) program, IBM, as an Advanced PartnerWorld Partner, and Serena. LogicLibrary has been recognized the past two years on the *SD Times* 100 list of leaders and innovators in the software development industry and has integration partnerships that include Microsoft, IBM, Eclipse and Borland. LogicLibrary is headquartered in Pittsburgh, with additional offices in Rochester, MN and Sunnyvale, CA. For more information, visit <http://www.logiclibrary.com>.

* Magic Quadrant for Metadata Repositories, 2004; Michael Blechar; March 5, 2004.

LogicLibrary and Logidex are trademarks of LogicLibrary, Inc.

All other brands and product names are trademarks or registered trademarks of their respective companies.

###