Trillian Vulnerabilities Open to Remote Exploitation

May 2 2007

Three flaws affecting the Trillian IM chat application that could lead to remote exploitation by hackers are fixed in new Trillian version.

Cerulean Studios has patched multiple vulnerabilities in its popular chat application that could have been exploited remotely by attackers.

Cerulean Studios are the makers of Trillian, an instant messaging consolidation application that supports IRC, ICQ, AIM and MSN protocols. In its latest version of Trillian, the company fixed three vulnerabilities in the IRC (Internet Relay Chat) module that could have been exploited remotely and given attackers the ability to intercept private conversations or execute code, security researchers at iDefense Labs reported.

Researchers at IM security provider Akonix Systems said the number of malicious code attacks over IM networks is on the rise. Akonix tracked 38 such attacks during April, including IM worms such as Pykse, Samo and Tiotua.

"Malware continues to be released through IM networks, and is on the rise again for the first time since January," said Don Montgomery, vice president of marketing at Akonix. "Businesses cannot ignore the liabilities and potential damage they are opening themselves up to with unmanaged IM applications and networks."

According to iDefense, it is possible to cause the Trillian IRC client to

return a malformed response to the server when handling long CTCP PING messages with UTF-8 characters. "This malformed response is truncated and is missing the terminating newline character," the iDefense advisory states. "This could allow the next line sent to the server to be improperly sent to an attacker."

In addition, whenever a user highlights a URL in an IRC message window, the chat application copies that data and places it in an internal buffer. If the URL contains a long string of UTF-8 characters, it is possible to overflow a heap-based buffer, corrupt memory and open the door for code execution, iDefense officials stated.

The final flaw allows a heap overflow to be triggered remotely when the IRC module receives a message that contains a font face HTML tag with the face attribute set to a long UTF-8 string. iDefense warns that attackers could use this vulnerability to intercept private communications for Trillian IRC users or execute code with the credentials of the currently logged on user.

The vulnerabilities affect Cerulean Studios Trillian 3.1, and have been addressed in Trillian version 3.1.5.0.