Yahoo Patches IM Vulnerability

April 6 2007

A buffer overflow problem is patched by the company.

Yahoo has patched a buffer overflow vulnerability in its instant-messaging tool that would have enabled attackers to potentially execute code on a compromised machine.

The flaw exists in an ActiveX control that is part of the Yahoo Messenger audio conference control. If exploited, a buffer overflow could cause a user to be involuntarily logged out of a chat or instant messaging session, the crash of an application such as Internet Explorer or the execution of code.

According to the company, an attacker would have to trick a user into viewing malicious HTML code in order for the attack to be successful.

Andrew Storms, director of security operations for San Francisco-based nCircle, said addressing the vulnerability could pose a problem in large corporate environments where Yahoo Messenger is widely used.

"Yahoo IM is heavily used in the corporate environment even if security policy doesn't officially permit it," he said. " - This vulnerability - leaves administrators with the choices to upgrade or set the kill-bit on the affected ActiveX control. Unfortunately, many corporations are unable to centrally manage upgrades - to - Windows Messenger, making this fix extremely time-intensive for IT teams. Many companies will be performing ad-hoc mitigation to get this cleaned up."

Yahoo advises anyone who has installed Yahoo Messenger before March 13 to install the update.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International