

FOR IMMEDIATE RELEASE:

The Building IT Company Works Overtime to Implement ActiveX Security Workaround

Jacksonville, FL – July 2009 – On Monday, July 6, 2009, Microsoft announced a Zero-Day vulnerability in ActiveX that could allow remote code execution on systems running Windows XP or Windows Server 2003. A Zero-day attack can occur when a window exists between the time a threat is found and when the security vendor releases the necessary patch. This remote code execution can occur when a user views a specially crafted Web page designed to exploit the vulnerability in Internet Explorer. Microsoft did not offer a patch but instead offered a manual workaround. The Building IT Company immediately started testing deployment methods to roll out this workaround to all client computers as quickly and safely as possible. After thoroughly testing, The Building IT Company deployed the workaround on thousands of client-supported computers nationally, overnight with no reported issues.

Over one week from the day the vulnerability was made public, Microsoft finally released the critical patch to address this flaw in ActiveX on Tuesday, July 14, 2009. Microsoft released a statement that included the following point: *“Customers who have (already) applied this workaround... do not need to install this security update.”* Since The Building IT Company has already applied the workaround to all supported client computers, no additional actions was necessary.

The Building IT Company’s CEO, Doug Lowenthal stated, *“The Building IT Company is proud to be ahead of the security curve when it comes to protecting our client’s data assets and making sure that we can maximize our client’s uptime by avoiding exploits like this from impacting their business. We know our clients appreciate our persistence and knowledge when it comes to protecting their company’s network.”*

Contact:

Info@BuildingITC.com

The Building IT Company

841 Prudential Drive, 12th Floor

Jacksonville, FL 32207

866-324-3324

<http://www.BuildingITC.com>

###