

TopResponse Threat Advisory

Release Date: May 9, 2007

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft BizTalk CAPICOM ActiveX Vulnerability (CVE-2007-0940).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft BizTalk Server 2004 SP1, Microsoft BizTalk Server 2004 SP2, CAPICOM, Platform SDK Redistributable: CAPICOM.

Alert Type: Targeted protection

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems.

Advisory Impact: Prevention

Summary: The Microsoft BizTalk CAPICOM ActiveX vulnerability could allow an attacker to execute arbitrary code on the user's system in the security context of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2007-05-08-02 (or later) to put this new protection into place. This is automatically applied to the "recommended" client protection ruleset. No further action is needed.

References: Use the following sources for additional information:

Additional Information	Location

Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS07-028.msp

Relevant TLN Rules: TLN-025070

Relevant TopResponse Protection Pack(s): 2007-05-08-02