

TopResponse Threat Advisory

Release Date: May 2, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft Works WkImgSrv.dll ActiveX Vulnerability (BID:28820).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Works 7 'WkImgSrv.dll', including v7.03.0616.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Works is an office suite that includes an imaging server component. There is a vulnerability in the component that can be exploited by instantiating an ActiveX control. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems 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:

IPS 5500 E-Series Users: Download and apply Protection Pack 2008-05-02-01 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, make sure the IPS rule tln-106187 is enabled in the IPS Rule Set used to inspect traffic initiated by your client infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.TopLayer.com/support
SecurityFocus Advisory	http://www.securityfocus.com/bid/28820

Relevant TLN Rules: tln-106187

Relevant TopResponse Protection Pack(s): 2008-05-02-01