



Top Layer's IPS 5500 Customers Automatically Protected Against Critical Microsoft Vulnerabilities

Westboro, MA, February 9, 2005 – Top Layer Networks, the global leader for high performance intrusion prevention solutions, today announced that its Attack Mitigator IPS™ 5500 intrusion prevention system already has the capability to protect customers from vulnerabilities disclosed yesterday by Microsoft in their vulnerability advisory without the need for any updates or configuration changes. The TopResponse™ research and development team considers two of these vulnerabilities to be serious threats to enterprise organizations. They are the License Logging Service Vulnerability (MS05-0010) and the Server Message Block Client Vulnerability (MS05-0011). Top Layer customers who deploy the Attack Mitigator IPS 5500 with recommended protection configurations are already protected against exploits of these vulnerabilities and need to take no further action.

Prior to the release of these Microsoft updates, the IPS 5500 has always been protecting customers from these vulnerabilities with its Microsoft Protocol Validation Module. Since Top Layer's protocol validation modules use protocol anomaly detection to inspect all transactions for acceptable use of the appropriate protocol, exploits of these critical vulnerabilities are automatically blocked regardless of the attack method used.

Peter Rendall, President and CEO of Top Layer Networks said, "Contrast this protection to other IPS vendors who rely primarily on distributing signatures to their customers after the vulnerability has been discovered. The exploit may have already disrupted operations by the time the signature is released. Even if a particular exploit is blocked under test conditions, their customers are highly vulnerable to common evasion techniques and the deluge of variants that spawn from an exploit as soon as it is released. Our customers know they can sleep at night with the confidence that our network-level and application-level protection is the most advanced and that they will remain protected ahead of future Microsoft patch releases."

Mike Paquette, VP, Product Management and Marketing of Top Layer stated, "Our intrusion prevention technology resonates well with customers who struggle to test and deploy patches on a timely basis. They understand that there are hundreds, maybe thousands of vulnerabilities not yet discovered that could have a potentially catastrophic impact on their business. We continue to see network traffic loads increase as businesses increase their reliance on the use of the Internet to conduct business. When combined with the increasing threat levels associated with the massive number of vulnerabilities that exist, proactive protection like that offered by Top Layer will become the industry standard for intrusion prevention systems."

The vulnerabilities included in the TopResponse advisory, issued on February 9, 2005 include the following:

Microsoft Advisory	CVE	Vulnerability
MS05-0004	CAN-2004-0847	ASP.net Vulnerability
MS05-0005	CAN-2004-0848	Office XP Vulnerability
MS05-0006	CAN-2005-0049	Sharepoint Cross-site Scripting and Spoofing Vulnerability
MS05-0007	CAN-2005-0051	Windows Named Pipe Vulnerability
MS05-0008	CAN-2005-0053	Drag-and-Drop Vulnerability
MS05-0009	CAN-2004-1244 CAN-2004-0597	PNG Processing Vulnerability
MS05-0010	CAN-2005-0050	License Logging Service Vulnerability
MS05-0011	CAN-2005-0045	Server Message Block Vulnerability
MS05-0012	CAN-2005-0047 CAN-2005-0044	OLE Input Validation Vulnerability
MS05-0013	CAN-2004-1319	DHTML Editing Component ActiveX Control Cross Domain Vulnerability
MS05-0014	CAN-2005-0053 CAN-2005-0054 CAN-2005-0055	Drag & Drop Vulnerability URL Decoding Zone Spoofing Vulnerability DHTML Method Heap Memory Corruption Vulnerability
MS05-0015	CAN-2005-0057	Hyperlink Object Library Vulnerability

For more information on the Microsoft vulnerabilities, click here:
<http://www.microsoft.com/technet/security/default.mspx>

About the Top Layer Attack Mitigator IPS 5500

The Attack Mitigator IPS 5500 family offers the strongest levels of Network IPS protection, performance and reliability on the market today. By improving upon the most powerful characteristics of stateful firewall technology and intrusion detection systems, Top Layer has developed the IPS 5500 in order to protect against attacks in real-time with minimal interruption of legitimate traffic. Top Layer executes high performance, non-disruptive deep packet inspection and analysis coupled with intelligent blocking of attacks through TopFire™ second-generation ASIC technology and TopInspect™ Deep Packet Inspection. To learn more about the Attack Mitigator IPS 5500, see our web site at www.toplayer.com or contact sales@TopLayer.com or call 508-870-1300.

About Top Layer Networks, Inc.

Founded in 1997, Top Layer Networks (www.TopLayer.com) develops network security solutions that enable enterprises worldwide to protect their infrastructure and critical online assets from cyber-threats. The Company's patented, ASIC-based products are engineered to deliver accurate and reliable protection mechanisms while operating as robust in-line network security devices. Top Layer Networks is headquartered in Westboro, Massachusetts with sales and support presence in Canada, France, Germany, Japan, Korea, the Netherlands and the United Kingdom.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact:

Donna Rogers	Matt Flanagan
Top Layer Networks	famaPR
Phone: 508-870-1300	Phone: 617-758-4141
Email: drogers@TopLayer.com	Email: matt@famapr.com