



CONTACT:

Kate Fly
TippingPoint, a division of 3Com
512.681.8218
kfly@tippingpoint.com

**TIPPINGPOINT PROTECTS CUSTOMERS FROM MICROSOFT
VULNERABILITIES DISCLOSED AND PATCHED TODAY**

Company's Digital Vaccine Service Preemptively Inoculates Networks from Attacks

MARLBOROUGH, Mass. – May 9, 2006 – TippingPoint, a division of 3Com and the leader in intrusion prevention, announced that its TippingPoint™ Intrusion Prevention Systems (IPS) provided complete protection against the vulnerabilities disclosed in all the bulletins announced by Microsoft today. The two most significant vulnerabilities were found in Microsoft's Exchange Server, which is widely deployed around the world, and in the Macromedia Flash Player installed by default on many Windows systems.

TippingPoint devices were inoculated against these threats through the Digital Vaccine® service, a remote update service that provides protection against the latest threats. TippingPoint provides vulnerability protection in the form of "Virtual Software Patches" to preemptively protect customers against exploits, malware and worms.

"The Exchange server remote code execution vulnerability is of extreme concern, as a specially crafted e-mail can potentially compromise a vulnerable Exchange Server," said Rohit Dhamankar, Manager of Security Research and Security Architect at TippingPoint. "The Macromedia Flash Player vulnerabilities can be exploited to install adware and spyware on a number of systems. Getting paid for infecting systems has become a new means of livelihood for criminals, and client-side threats like these vulnerabilities are a vehicle for such infections. I believe the TippingPoint IPS, with a comprehensive protection for server as well as client vulnerabilities, is the best way to protect any IP network."

The TippingPoint IPS provides protection for the following security bulletins announced by Microsoft today:

(1) *MS06-018*

Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service

(Rating: Moderate)

(2) *MS06-019*

Vulnerability in Microsoft Exchange Could Allow Remote Code Execution

(Rating: Critical)

(3) *MS06-020*

Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution

(Rating: Critical)

For more information on the Microsoft vulnerabilities, please visit:

<http://www.microsoft.com/technet/security/bulletin/ms06-may.msp>.

About TippingPoint, a division of 3Com

TippingPoint, a division of 3Com, is the leading provider of network-based intrusion prevention systems. The TippingPoint IPS is the most decorated in its industry. For a full list of awards, visit http://www.tippingpoint.com/products_certifications.html. Our innovative approach offers customers unmatched network-based security with ultra-high performance, scalability and reliability. TippingPoint is based in Austin, Texas, and can be contacted through its Web site at www.tippingpoint.com or by telephone at 1-888-TRUE-IPS.

About 3Com Corporation

3Com Corporation (NASDAQ: COMS) is a leading provider of secure, converged voice and data networking solutions for enterprises of all sizes. 3Com offers a broad line of innovative products backed by world class sales, service and support, which excel at delivering business value for its customers. Through its TippingPoint division, 3Com is the leading provider of network-based intrusion prevention systems that deliver in-depth application protection, infrastructure protection, and performance protection. 3Com also is the majority owner of Huawei-3Com Co., Ltd. (H-3C), a China-based joint venture formed by 3Com and Huawei in November 2003. H-3C brings innovative and cost-effective product development and manufacturing and a strong footprint in one of the world's most dynamic markets. For further information, please visit www.3com.com, or the press site www.3com.com/pressbox.

Copyright © 2006 3Com Corporation. 3Com, the 3Com logo and Digital Vaccine are registered trademarks and TippingPoint is a trademark of 3Com Corporation or its subsidiaries. All other company and product names may be trademarks of their respective holders.

###