



CONTACT:

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

**FROST & SULLIVAN RESEARCH SHOWS TIPPINGPOINT LEADS IN
DISCOVERY OF BOTH HIGH SEVERITY AND MICROSOFT FLAWS**

*TippingPoint Success Attributed to Internal DV Labs Researchers and Zero Day Initiative
Program*

SAN FRANCISCO – 2007 RSA CONFERENCE BOOTH #1616 – Feb. 6, 2007 –

TippingPoint, the leader in intrusion prevention, today announced that its research organization, DV Labs, was recognized as the fastest growing discoverer of new vulnerabilities and the leader in the discovery of high-severity and Microsoft vulnerabilities by recent Frost & Sullivan research.

This research, titled “Analysis of Vulnerability Discovery and Disclosure,” tracks vulnerability discoveries and their severity level from January 2005 to September 2006 by correlating research from the US-CERT vulnerability database, the National Vulnerability Database (NVD), SecurityFocus, and other public sources. Frost & Sullivan’s analysis uses the rankings of the Common Vulnerability Scoring System (CVSS) used by the NVD as a basis for severity level of the threats. By correlating information from the most widely recognized vulnerability databases and scoring systems, Frost & Sullivan’s report clearly shows that TippingPoint’s DV Labs discovered more high severity vulnerabilities than any other research firm.

TippingPoint’s DV Labs consists of a large team of recognized internal TippingPoint researchers as well as over 400 researchers from its Zero Day Initiative (ZDI), an external research program launched in the summer of 2005 to enable the responsible disclosure of vulnerabilities and give TippingPoint Intrusion Prevention System customers advanced protection for zero day threats. Through its researchers,

TippingPoint was responsible for the discovery of over 100 vulnerabilities in 2006, 23 of which were Microsoft vulnerabilities. TippingPoint customers were protected from these zero day issues well in advance of attacks.

According to Rob Ayoub, industry manager at Frost & Sullivan, “During the first three quarters of 2006, companies that leveraged in-house research with external talent were the most successful in discovering high-severity vulnerabilities. Through initiatives like DV Labs, TippingPoint is able to provide timely discovery, comprehensive development, and rapid delivery of vulnerability remediation to its enterprise customers.”

Organizations face more threats today than ever before. The Frost & Sullivan research points to the increasing number of vulnerabilities and the shrinking window between vulnerability and exploit. In addition, there is the newer threat of zero day attacks. A zero day vulnerability is one that is unknown or one that has been publicly disclosed without a corresponding patch, leaving organizations with few solutions to protect themselves against attacks. IPS is one of the few solutions able to provide zero day protection. In 2006, 19 zero day vulnerabilities were disclosed without a patch, according to the report.

Through its ZDI program, TippingPoint rewards security researchers for responsibly informing TippingPoint of newly discovered zero day vulnerabilities. TippingPoint notifies the affected vendor so a patch can be developed and the researcher agrees to keep the information confidential until the patch is issued so affected organizations are not at risk of attack. In addition to protecting all users from zero day threats by ensuring potentially harmful information is kept confidential until a solution is available, TippingPoint customers are protected against exploits of zero day vulnerabilities through security filters delivered through the Digital Vaccine® service. Further, through its stewardship with other vendors and research organizations, TippingPoint extends the benefit of its vulnerability discovery intelligence to the security industry, which helps drive network security excellence for many businesses.

To view the full Frost & Sullivan report, please visit:

http://www.tippingpoint.com/resources_whitepapers.html

About TippingPoint, a division of 3Com

TippingPoint, the leader in intrusion prevention systems (IPS), provides the IPS-secured network, which delivers attack control, access control, and application control. Its foundation is the TippingPoint IPS, the most decorated in its industry with unparalleled performance and security, as evidenced by nearly 35 awards. For a full list, visit: http://www.tippingpoint.com/products_certifications.html. The IPS obtains evergreen protection from the Digital Vaccine service, powered by DV Labs, the largest body of security researchers in the world. DV Labs is made up of expert internal researchers and over 400 Zero Day Initiative researchers. For more information on TippingPoint, please visit: www.tippingpoint.com or call 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 China-based Huawei-3Com Co., Ltd. (H3C). On November 28, 2006, 3Com announced that the company reached an agreement to acquire Huawei's remaining 49 percent stake and take full ownership, pending customary approvals. H3C 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 © 2007 3Com Corporation. 3Com, Digital Vaccine and the 3Com logo 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.

###