



MEDIA CONTACTS:

Jennifer Lake
TippingPoint
+1 512-681-8111
jlake@tippingpoint.com

Michelle Dillon
Beaupre
+1 603-559-5835
mdillon@beaupre.com

Independent Report Shows TippingPoint Leads Industry in Software Vulnerability Discoveries

Security Intelligence from DV Labs, Zero Day Initiative Drives Faster Filter Development and Improved Network Protection

AUSTIN, TX – January 19, 2010 – According to the most recent Frost & Sullivan Vulnerability Tracker, [TippingPoint](#), a leader in network security and a division of 3Com, continues to lead the industry in security research. The report, which highlights software vulnerabilities discovered in the first half of 2009, credits TippingPoint with finding more vulnerabilities than any other research organization it tracks. To this end, TippingPoint has also announced that for the entire year, it has uncovered 114 vulnerabilities that threatened the most common browsers, operating systems and Web applications, as well as increased the number of external contributors to its Zero Day Initiative (ZDI) program to over 1,100. The research culled from these vulnerabilities is built into the filters and signatures that keep the TippingPoint® Intrusion Prevention System (IPS) Platform up-to-date and customers protected against the latest security threats.

Security threats continued to evolve in 2009, both in the objects targeted and the methods used for exploitation. Common business applications such as PDF document readers and Internet browsers continued to attract hackers with their large attack surface and enticing profit potential. Attacks targeted at custom Web applications also increased this past year due to increased use in the enterprise world. Worms like Conficker, which dominated the security attack landscape in 2009, show that hackers are using multiple vectors to exploit these vulnerabilities as well as going to great lengths to succeed with their attacks.

Published in December 2009, the Frost & Sullivan Vulnerability Tracker for 1H2009 included a number of key findings that demonstrate TippingPoint's leadership in vulnerability research, including:

- TippingPoint reported more than twice the number of media application vulnerabilities than its next closest competitor.
- TippingPoint found more than twice the browser vulnerabilities than any other research organization.
- Heap-based overflows were the most common type of vulnerability reported and TippingPoint led the market in reporting these vulnerabilities.
- More than 82.5 percent of reported vulnerabilities enabled the attacker to take full control of the compromised system. These systems can be used by criminals for activities such as denial-of-service attacks, spam messaging, or phishing attacks. TippingPoint led all researchers by reporting the highest number of vulnerabilities that enabled this type of code execution.

“Hacking has evolved from simple glory-seeking missions to a complex business model that rivals the organizational structure of today’s most successful enterprises. The profit potential has bred a new class of cybercriminal, making it even more important to keep ahead the attacks,” said David Endler, senior director of security research at TippingPoint. “In general, the number of people with the skills to discover vulnerabilities is increasing. However, with programs like ZDI, we are seeing a measurable increase in the number of talented researchers willing to work on the right side of the law.”

TippingPoint’s Digital Vaccine[®] Labs (DVLabs) security research team is the benchmark of vulnerability and security research in the industry. Providing the security intelligence behind TippingPoint’s products, the DVLabs team consists of world-renowned internal security researchers that apply their cutting-edge engineering and analysis talents in their daily operations. In 2005, TippingPoint founded the ZDI, a program which rewards external researchers for responsibly reporting discovered vulnerabilities. Since its inception the program has grown to more than 1,100 researchers from countries across the globe.

The success of TippingPoint’s vulnerability research and reporting program has been bolstered by the explosive growth of researchers contributing to the ZDI program, as well as the increase in vulnerabilities being reported, according to Robert Ayoub, industry manager for Frost & Sullivan North America. “For the last several years, we’ve been tracking the vulnerabilities reported by vendors and research organizations to get a better sense of the security risks that are out there. Over the years, we’ve seen the bulk of reporting shift from the vendors and private sources to third-party research organizations like TippingPoint’s ZDI program. TippingPoint has been

particularly successful in recent years having put up an impressive quarter-over-quarter increase in reported vulnerabilities since 2008, surpassing all of the other organizations to lead market.”

“The report from Frost & Sullivan really demonstrates that the research from DV Labs and the ZDI program is unrivaled in the industry. The recent attacks on Google using a vulnerability in Internet Explorer are a prime example of the types of vulnerabilities our researchers have been uncovering for several years,” added Endler. “Discovering and understanding these vulnerabilities are what make the Digital Vaccine service such a differentiator for TippingPoint. The depth of the research coming out of both ZDI and DV Labs is what allows us to provide such comprehensive security coverage in the IPS.”

For more information on TippingPoint’s security research, visit the DV Labs Web site at <http://dvlabs.tippingpoint.com> or the Zero Day Initiative Web site at <http://www.zerodayinitiative.com>.

About TippingPoint and 3Com

[TippingPoint](http://www.tippingpoint.com) is the enterprise security brand of 3Com Corporation (NASDAQ: COMS), a \$1.3 billion global enterprise networking solutions provider that sets a new price/performance standard for customers. 3Com has three global brands—[H3C](http://www.h3c.com), [3Com](http://www.3com.com), and [TippingPoint](http://www.tippingpoint.com)—that offer high-performance networking and security solutions to enterprises large and small. TippingPoint leads the advancement of network security with a modern network security platform and intrusion prevention system (IPS), purpose-built to protect today’s next-generation data center network from evolving, global security threats. TippingPoint helps organizations reduce security operating costs while ensuring maximum business continuity. For more information on TippingPoint, please visit www.tippingpoint.com, or the press center at www.tippingpoint.com/press.

Copyright © 2010 3Com Corporation. 3Com, 3Com logo, H3C, H3C logo, Digital Vaccine and TippingPoint are registered trademarks of 3Com Corporation or its wholly owned subsidiaries in various countries throughout the world. All other company and product names may be trademarks of their respective holders.

###