



CONTACT:

Laura Craddick
TippingPoint, a division of 3Com
512.708.9706
Laura_craddick@3com.com

**TIPPINGPOINT MARKS ONE YEAR ANNIVERSARY OF ZERO DAY
INITIATIVE BY UNVEILING DISCLOSURE PIPELINE**

*30 Zero Day Vulnerabilities Eliminated Through Program; 29 Issues Pending; Over 400
Security Researchers Signed Up*

AUSTIN, TX. – August 28, 2006 –TippingPoint, a division of 3Com and the leader in intrusion prevention, today marked the one year anniversary of the Zero Day Initiative (ZDI) inception by announcing it will begin publishing statistics on all vulnerabilities pending public disclosure on the Zero Day Initiative Web site, www.zerodayinitiative.com. These 29 unresolved issues have been reported to the Zero Day Initiative, and are currently being addressed by the affected vendors.

In order to reduce the risk of exploitation, the only vulnerability details published are the vendor name, the date TippingPoint reported the threat to the affected vendor, and the severity level. No technical details are shared about the vulnerability or the name of the vendor's specific product in order to protect exposed users of the affected vendor. TippingPoint™ Intrusion Prevention System customers were preemptively protected against pending zero day vulnerabilities within days of reporting the issue to the affected vendor.

Since launching the Zero Day Initiative portal last August, 30 zero day threats have been addressed by ensuring details regarding unknown or undisclosed vulnerabilities remained confidential until the issue could be disclosed with the affected vendor's solution or patch. Of these 30 issues, seven involve widely used Microsoft software products. Other Zero Day Initiative vulnerabilities over the last year have also affected vendors including Mozilla, Symantec, Novell, Adobe, and Apple to name a few.

Over 400 security researchers are now signed up to the ZDI program, in addition to the original research being performed by the TippingPoint security research team (TSRT). The TSRT shares statistics of its pending vulnerability advisories on the TippingPoint site, and has discovered 16 zero day vulnerabilities over the last year, including three Microsoft issues. Six of the issues discovered by TippingPoint researchers are still awaiting a vendor-issued solution, which are published here: http://www.tippingpoint.com/security/upcoming_advisories.html.

“Over the past year, the most resounding suggestion from our Zero Day Initiative researchers was to add more transparency to our program by publishing the pipeline of vendors with pending zero day vulnerabilities,” said David Endler, director of security research for TippingPoint. “We've been pleased with the progress we have made acting as an intermediary between security vendors and researchers, ultimately working together to help protect the vendor's customers from emerging zero-day exploits while appropriately rewarding the researcher.”

The Zero Day Initiative was launched by 3Com and its TippingPoint division to enable the responsible disclosure of vulnerabilities in order to make technology more secure for users and businesses. A zero day vulnerability is one that is unknown or one that has been publicly disclosed without a corresponding patch or solution.

Through the program, 3Com rewards security researchers for responsibly informing 3Com of newly discovered zero day vulnerabilities. 3Com 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 patch is issued, TippingPoint customers are protected against exploits of zero day vulnerabilities through security filters delivered through the Digital Vaccine® service.

For a full list of the 30 ZDI advisories where a vulnerability has been patched by the vendor, please visit: <http://www.zerodayinitiative.com/advisories.html>. For a list of vulnerabilities discovered by TippingPoint security research team, please visit: http://www.tippingpoint.com/security/published_advisories.html.

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 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.

###