



CONTACT:

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

TIPPINGPOINT DISCOVERS ISSUE IN MICROSOFT BULLETIN, PROTECTS CUSTOMERS FROM VULNERABILITIES DISCLOSED AND PATCHED TODAY

Company's Zero Day Initiative Researcher Finds Flaw in Microsoft Internet Explorer

AUSTIN, TX. – November 14, 2006 – TippingPoint, a division of 3Com and the leader in intrusion prevention, announced that its TippingPoint™ Intrusion Prevention Systems (IPS) provide complete protection against all vulnerabilities disclosed in the bulletins announced by Microsoft today, including one vulnerability discovered by its own Zero Day Initiative.

Microsoft security bulletin MS06-067 includes fixes for multiple zero day vulnerabilities affecting Microsoft Internet Explorer which typically target end users and can be used to create bot networks. One of the issues was discovered and reported through TippingPoint's Zero Day Initiative on July 18, 2006. The Zero Day Initiative has uncovered 11 vulnerabilities affecting Microsoft products to date with an additional seven outstanding issues listed at:

http://www.zerodayinitiative.com/upcoming_advisories.html.

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.

“Today's Microsoft bulletins demonstrate a consistent trend of response to zero-day exploits discovered in the wild,” said Dave Endler, director of security research at

TippingPoint. “TippingPoint researchers have noticed an increase in malicious activity from Eastern European attackers that leverage these privately discovered vulnerabilities affecting Internet Explorer and Microsoft Office. This growing trend was a strong factor behind the launch of TippingPoint's Zero Day Initiative.”

The goal of the Zero Day Initiative is 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. Through the program, 3Com rewards security researchers for responsibly informing 3Com 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 to mitigate risks to affected organizations. In addition to protecting all users from zero day threats by ensuring information is kept confidential until a patch is issued, TippingPoint’s customers are protected against zero day attacks through security filters delivered through the Digital Vaccine service.

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

(1) MS06-066

*Vulnerabilities in Client Service for Netware Could Allow Remote Code Execution
CVE-2006-4688, CVE-2006-4689*

(Rating: Important)

(2) MS06-067

*Cumulative Security Update for Internet Explorer
CVE-2006-4687, CVE-2006-4446, CVE-2006-4777*

(Rating: Critical)

(3) MS06-068

*Vulnerability in Microsoft Agent Could Allow Remote Code Execution
CVE-2006-3445*

(Rating: Critical)

(4) MS06-069

*Vulnerabilities in Macromedia Flash Player Could Allow Remote Code Execution
CVE-2006-3014, CVE-2006-3311, CVE-2006-3587, CVE-2006-3588, CVE-2006-4640*

(Rating: Critical)

(5) MS06-070

Vulnerability in Workstation Service Could Allow Remote Code Execution

CVE-2006-4691

(Rating: Critical)

(6) MS06-071

Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution

CVE-2006-5745

(Rating: Critical)

For more information on the Microsoft vulnerabilities, please visit:

<http://www.microsoft.com/technet/security/bulletin/ms06-nov.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.

###