



CONTACT:

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

3COM'S SECURITY TEAM AND ZERO DAY INITIATIVE DISCOVER CRITICAL MICROSOFT VULNERABILITIES

3Com Provides Customers with Same Day Protection Against Critical Microsoft Bulletins Disclosed Today

MARLBOROUGH, Mass. – August 8, 2006 – 3Com and its TippingPoint division today announced that its security research team discovered three critical Microsoft vulnerabilities that were fixed today. Additionally, 3Com's Zero Day Initiative (ZDI) discovered two additional critical Microsoft vulnerabilities in Internet Explorer that were also fixed.

Upon validating the vulnerabilities, 3Com reported the issues to Microsoft, which in turn applied the necessary resources to address the vulnerabilities and issue patches today. 3Com customers using the TippingPoint™ Intrusion Prevention Systems (IPS) were preemptively protected against potential zero day attacks targeting the vulnerabilities through its Digital Vaccine® update service.

The vulnerabilities (CVE-2006-3357, CVE-2006-3086, CVE-2006-3638), discovered by members of the TippingPoint Security Research Team (TSRT), allow remote attackers to execute arbitrary code on vulnerable installations of the Microsoft Windows operating system upon visiting a malicious website. The critical Internet Explorer vulnerabilities (CVE-2006-3450, CVE-2006-3451), discovered through the ZDI Program, also allows remote attackers to execute arbitrary code if a malicious website is visited by a victim.

The TSRT consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in our daily operations. The by-product of these efforts fuels the creation of vulnerability filters that are

automatically delivered to TippingPoint customers through the Digital Vaccine service. For more information about TSRT, please visit: <http://www.tippingpoint.com/security>

The goal of the ZDI program 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. Once its security experts validate the authenticity of the vulnerability, 3Com notifies the affected vendor so a patch can be developed. The researcher agrees to keep the information confidential until the patch is issued so affected organizations are not at risk. In addition to protecting all users from zero day threats by ensuring information is kept confidential until a patch is issued, TippingPoint customers are also protected against zero day attacks through security filters delivered through the Digital Vaccine service.

In addition to protecting customers from the five aforementioned vulnerabilities, TippingPoint Intrusion Prevention Systems were inoculated against issues in the following Microsoft bulletins through the Digital Vaccine service:

(1) MS06-040

Vulnerability in Server Service Could Allow Remote Code Execution
(Rating: Critical)

(2) MS06-041

Vulnerability in DNS Resolution Could Allow Remote Code Execution
(Rating: Critical)

(3) MS06-042

Cumulative Security Update for Internet Explorer
(Rating: Critical)

(4) MS06-043

Vulnerability in Microsoft Windows Could Allow Remote Code Execution
(Rating: Critical)

(5) MS06-044

Vulnerability in Microsoft Management Console Could Allow Remote Code Execution
(Rating: Critical)

(6) MS06-045

Vulnerability in Windows Explorer Could Allow Remote Code Execution
(Rating: Critical)

(7) MS06-046

Vulnerability in HTML Help Could Allow Remote Code Execution

(Rating: Critical)

(8) MS06-047

Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution

(Rating: Critical)

(9) MS06-048

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution

(Rating: Critical)

(10) MS06-050

Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution

(Rating: Important)

For more information on the Microsoft vulnerabilities, please visit:

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

For a full list of TippingPoint Security Research Team advisories, please visit

<http://www.tippingpoint.com/security>

For a full list of ZDI advisories and specific information on the Microsoft vulnerabilities, please visit: <http://www.zerodayinitiative.com/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, 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.

###