



**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 All Critical Microsoft Bulletins Disclosed Today*

**MALBOROUGH, Mass. – July 11, 2006** – 3Com and its TippingPoint division today announced that its security research team discovered a critical vulnerability in Microsoft Windows operating system. Additionally, 3Com's Zero Day Initiative (ZDI) discovered another critical Microsoft vulnerability in its Excel software.

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

The critical vulnerability (CVE-2006-1314), discovered by the TippingPoint Security Research Team (TSRT), allows remote attackers to execute arbitrary code on vulnerable installations of the Microsoft Windows operating system. This vulnerability can lead to a network worm that could have a widespread impact. The critical vulnerability (CVE-2006-2388), discovered through the ZDI, allows remote attackers to execute arbitrary code if a malformed Excel spreadsheet is opened by a victim.

The TSRT consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in TippingPoint's 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 the TippingPoint Security Research Team, 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, and 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 two aforementioned vulnerabilities, TippingPoint Intrusion Prevention Systems were inoculated against issues in all of today's critical Microsoft bulletins through the Digital Vaccine service. The TippingPoint IPS provides protection for the following security bulletins announced by Microsoft today:

(1) *MS06-033*

Vulnerability in ASP.NET Could Allow Information Disclosure

*(Rating: Important)*

(2) *MS06-035*

Vulnerability in Server Service Could Allow Remote Code Execution

*(Rating: Critical)*

(3) *MS06-036*

Vulnerability in DHCP Client Service Could Allow Remote Code Execution

*(Rating: Critical)*

(4) *MS06-037*

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution

*(Rating: Critical)*

(5) *MS06-038*

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution

*(Rating: Critical)*

(6) MS06-039

Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution

(Rating: Critical)

For more information on the Microsoft vulnerabilities, please visit:

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

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

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

For a full list of ZDI advisories, 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](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](http://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](http://www.3com.com), or the press site [www.3com.com/pressbox](http://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.

###