



**CONTACT:**

Kate Fly  
TippingPoint  
512.681.8218  
kfly@tippingpoint.com

**TIPPINGPOINT DISCOVERS TWO FLAWS IN MICROSOFT BULLETINS  
RELEASED TODAY**

**AUSTIN, Texas – May 8, 2007** –TippingPoint, the leader in intrusion prevention, today announced that it is responsible for the discovery of two flaws released in today’s Microsoft Bulletins due to its Zero Day Initiative (ZDI) global researcher network. TippingPoint™ Intrusion Prevention Systems (IPS) also provide complete protection against all vulnerabilities disclosed in today’s Microsoft bulletins.

The first vulnerability uncovered by the Zero Day Initiative, MS07-027, affects Internet Explorer and could allow an attacker to execute arbitrary code on vulnerable installations. The second issue uncovered by the ZDI this month, MS07-023, affects Microsoft Office Excel, and could also lead to arbitrary code execution if a user opens a malicious .xls file. TippingPoint IPS customers have been preemptively protected against both flaws.

TippingPoint also protected its customers’ networks from another zero-day buffer overflow affecting Microsoft DNS servers. This vulnerability, being patched by Microsoft Security Bulletin MS07-029 today, has been exploited in the wild since April 12, 2007. “Compromising a DNS server can be exploited for large scale malware deployment on computer systems by redirecting users to attacker-controlled domains,” said Rohit Dhamankar, senior research manager of TippingPoint’s DV Labs. “With the rise in zero-day and targeted attacks, the importance of virtual patching via intrusion prevention systems cannot be over-emphasized.”

TippingPoint Intrusion Prevention Systems were inoculated against the issues in today's Microsoft bulletins through the Digital Vaccine® service. The TippingPoint IPS provides protection for the following security bulletins announced by Microsoft today:

(1) MS07-023

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution  
(Rating: Critical)

(2) MS07-024

Vulnerabilities in Microsoft Word Could Allow Remote Code Execution  
(Rating: Critical)

(3) MS07-025

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

(4) MS07-026

Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution  
(Rating: Critical)

(5) MS07-027

Cumulative Security Update for Internet Explorer  
(Rating: Critical)

(6) MS07-028

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

(7) MS07-029

Vulnerability in RPC on Windows DNS Server Could Allow Remote Code Execution  
(Rating: Critical)

For more information on the Microsoft vulnerabilities, please visit:

<http://www.microsoft.com/technet/security/bulletin/ms07-may.msp>

#### **About TippingPoint, a division of 3Com**

TippingPoint, the leader in intrusion prevention systems (IPS), provides the IPS-secured network, which delivers attack control, access control, and application control. Its foundation is the TippingPoint IPS, the most decorated in its industry with unparalleled performance and security, as evidenced by nearly 35 awards. For a full list, visit: [http://www.tippingpoint.com/products\\_certifications.html](http://www.tippingpoint.com/products_certifications.html). The IPS obtains evergreen protection from the Digital Vaccine service, powered by DVLabs, the largest body of security researchers in the world. DVLabs is made up of expert internal researchers and over 400 Zero Day Initiative researchers. For more information on TippingPoint, please visit: [www.tippingpoint.com](http://www.tippingpoint.com) or call 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 owns H3C Technologies Co., Limited (H3C), a China-based provider of network infrastructure products. H3C 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 © 2007 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.

###