Microsoft Windows URI Handling Command Execution Vulnerability

2007-07-26 19:01:18 by raven

SECUNIA ADVISORY ID: SA26201

VERIFY ADVISORY: http://secunia.com/advisories/26201/

CRITICAL: Highly critical

IMPACT: System access

WHERE: >From remote

OPERATING SYSTEM:
Microsoft Windows XP Professional - http://secunia.com/product/22/
Microsoft Windows XP Home Edition - http://secunia.com/product/16/
Microsoft Windows Server 2003 Datacenter Edition - http://secunia.com/product/1175/
Microsoft Windows Server 2003 Enterprise Edition - http://secunia.com/product/1174/
Microsoft Windows Server 2003 Standard Edition - http://secunia.com/product/1173/
Microsoft Windows Server 2003 Web Edition - http://secunia.com/product/1176/

SOFTWARE: Microsoft Internet Explorer 7.x - http://secunia.com/product/12366/

DESCRIPTION: A vulnerability has been discovered in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system. Successful exploitation requires that Internet Explorer 7 is installed on the system.

The vulnerability is caused due to an input validation error within the handling of system default URIs with registered URI handlers (e.g. "mailto", "news", "nntp", "snews", "telnet"). This can be exploited to execute arbitrary commands when a user e.g. using Firefox visits a malicious website with a specially crafted "mailto" URI containing a "%" character and ends in a certain extension (e.g. ".bat", ".cmd")

Examples: mailto:test%windows/system32/calc.exe".cmd nntp:Windows/system32/telnet.exe" "secunia.com 80%.bat

The vulnerability is confirmed on a fully patched Windows XP SP2 and Windows Server 2003 SP2 system using Firefox version 2.0.0.5 and Netscape Navigator version 9.0b2. Other versions and browsers may also be affected.

SOLUTION: Do not browse untrusted websites or follow untrusted links.

PROVIDED AND/OR DISCOVERED BY:
Vulnerability discovered by: * Billy (BK) Rios
Firefox not escaping quotes originally discussed by: * Jesper Johansson
Additional research by Secunia Research.

ORIGINAL ADVISORY: Billy (BK) Rios: http://xs-sniper.com/blog/2007/07/24/remote-command-execution-in-firefox-2005/

OTHER REFERENCES:
US-CERT VU#783400: http://www.kb.cert.org/vuls/id/783400
Jesper Johansson blog: http://msinfluentials.com/blogs/jesper/archive/2007/07/20/hey-mozilla-quotes-are-not-legal-in-a-url.aspx