

Microsoft Windows Win32 API Code Execution Vulnerability

2007-06-12 17:28:23 by Raven

SECUNIA ADVISORY ID: SA25640

VERIFY ADVISORY: <http://secunia.com/advisories/25640/>

CRITICAL: Highly critical

IMPACT: Privilege escalation, System access

WHERE: >From remote

OPERATING SYSTEM:

Microsoft Windows 2000 Professional - <http://secunia.com/product/1/>

Microsoft Windows XP Home Edition - <http://secunia.com/product/16/>

Microsoft Windows XP Professional - <http://secunia.com/product/22/>

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/>

Microsoft Windows Storage Server 2003 - <http://secunia.com/product/12399/>

DESCRIPTION: A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges or by malicious people to compromise a user's system.

The vulnerability is caused due to an input validation error in the Win32 API when handling parameters to a function call. This can be exploited to execute arbitrary code via a local application using the vulnerable component or when a user e.g. views a specially crafted web page using Internet Explorer.

SOLUTION: Apply patches.

Windows 2000 SP4: <http://www.microsoft.com/downloads/details.aspx?FamilyId=3918ac76-ebb6-4886-9a9e-808eafb96b1b>

Windows XP SP2: <http://www.microsoft.com/downloads/details.aspx?FamilyId=27c7f1b9-2d1d-40cb-ad7e-bfedb6156a9c>

Windows XP Professional x64 Edition (optionally with SP2): <http://www.microsoft.com/downloads/details.aspx?FamilyId=0ba12191-1e6f-443b-9150-7ab8b2deb7c2>

Windows Server 2003 SP1/SP2: <http://www.microsoft.com/downloads/details.aspx?FamilyId=d554dff4-bcfb-4bbc-8fa0-af2f939d2610>

Windows Server 2003 x64 Edition (optionally with SP2): <http://www.microsoft.com/downloads/details.aspx?FamilyId=170473d8-6bb1-4fbd-8494-a059dbfdf182>

Windows Server 2003 with SP1/SP2 for Itanium-based systems: <http://www.microsoft.com/downloads/details.aspx?FamilyId=f5e45e3c-4cac-41a5-99f7-42c2c2c73e99>

PROVIDED AND/OR DISCOVERED BY: The vendor credits Billy Rios, VeriSign.

ORIGINAL ADVISORY: MS07-035 (KB935839):

<http://www.microsoft.com/technet/security/bulletin/ms07-035.msp>

<https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2955>