

Microsoft MDAC ADODB.Connection ActiveX Control Vulnerability

2007-02-13 19:15:53 by Raven

SECUNIA ADVISORY ID: SA22452

VERIFY ADVISORY: <http://secunia.com/advisories/22452/>

CRITICAL: Highly critical

IMPACT: DoS, 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 Web Edition - <http://secunia.com/product/1176/>

Microsoft Windows Server 2003 Standard Edition - <http://secunia.com/product/1173/>

Microsoft Windows Server 2003 Enterprise Edition - <http://secunia.com/product/1174/>

Microsoft Windows Server 2003 Datacenter Edition - <http://secunia.com/product/1175/>

Microsoft Windows 2000 Server - <http://secunia.com/product/20/>

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

Microsoft Windows 2000 Datacenter Server - <http://secunia.com/product/1177/>

Microsoft Windows 2000 Advanced Server - <http://secunia.com/product/21/>

SOFTWARE: Microsoft Data Access Components (MDAC) 2.x <http://secunia.com/product/1807/>

DESCRIPTION: Yag Kohha has reported a vulnerability in Microsoft Data Access Components, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the ADODB.Connection ActiveX control when handling the "Execute()" method. This can be exploited to cause a memory corruption by passing specially crafted parameters to the method. Successful exploitation may allow execution of arbitrary code when a user e.g. visits a malicious website.

SOLUTION: Apply patches.

MDAC 2.5 SP3 on Windows 2000 SP4: <http://www.microsoft.com/downloads/details.aspx?FamilyId=EF163E3E-DD3B-4429-98A4-720DA2C96464>

MDAC 2.8 SP1 on Windows XP SP2: <http://www.microsoft.com/downloads/details.aspx?FamilyId=6B0CDB65-AEF4-489F-B917-812D9F7687BD>

MDAC 2.8 on Windows Server 2003: <http://www.microsoft.com/downloads/details.aspx?FamilyId=34D24335-4EC0-49E7-9E3F-787F89DD7B1D>

MDAC 2.8 on Windows Server 2003 for Itanium-based systems: <http://www.microsoft.com/downloads/details.aspx?FamilyId=58322D1B-A1A8-4BA6-BA1B-6649013CC324>

MDAC 2.7 SP1 installed on Windows 2000 SP4: <http://www.microsoft.com/downloads/details.aspx?FamilyId=591B0967-C8AB-4B85-A9AF-C01E8D8E3ADC>

MDAC 2.8 installed on Windows 2000 SP4: <http://www.microsoft.com/downloads/details.aspx?FamilyId=BC864245-175A-4B55-AB4A-FB5D0E03DCFC>

MDAC 2.8 SP1 installed on Windows 2000 SP4: <http://www.microsoft.com/downloads/details.aspx?FamilyId=341859BF-8DAA-419B-88CD-E5E8EB4A5BAD>

PROVIDED AND/OR DISCOVERED BY: Yag Kohha - The vendor also credits Frsirt.

ORIGINAL ADVISORY: MS07-009 (KB927779):

<http://www.microsoft.com/technet/security/Bulletin/MS07-009.msp>

OTHER REFERENCES: US-CERT VU#589272: <http://www.kb.cert.org/vuls/id/589272>

<https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2752>