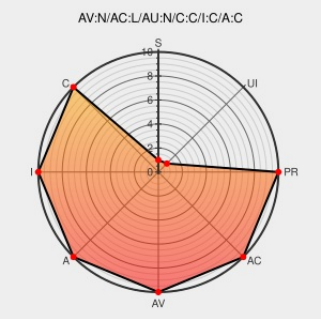
CVE-2007-1512

Published on: 03/20/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:35 PM UTC

CVE-2007-1512

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Visual Studio .net from Microsoft contain the following vulnerability:

Stack-based buffer overflow in the AfxOleSetEditMenu function in the MFC component in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 Gold and SP1, and Visual Studio .NET 2002 Gold and SP1, and 2003 Gold and SP1 allows user-assisted remote attackers to have an unknown impact (probably crash) via an RTF file with a malformed OLE object, which results in writing two 0x00 characters past the end of szBuffer, aka the "MFC42u.dll Off-by-Two Overflow." NOTE: this issue is due to an incomplete patch (MS07-012) for CVE-2007-0025.

CVE-2007-1512 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070316 MS07-012 Not Fixed

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visual Studio .net	2002	gold	All	All
Application	Microsoft	Visual Studio .net	2002	sp1	All	All
Application	Microsoft	Visual Studio .net	2003	gold	All	All
Application	Microsoft	Visual Studio .net	2003	sp1	All	All
Application	Microsoft	Visual Studio .net	2002	gold	All	All
Application	Microsoft	Visual Studio .net	2002	sp1	All	All
Application	Microsoft	Visual Studio .net	2003	gold	All	All
Application	Microsoft	Visual Studio .net	2003	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	gold	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	gold	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All

cpe:2.3:a:microsoft:visual_studio_.net:2002:gold:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2002:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2003:gold:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2003:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2002:gold:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2002:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2003:gold:*:*:*:*:*:*:

cpe:2.3:a:microsoft:visual_studio_.net:2003:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:gold:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:sp1:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:gold:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:sp1:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→