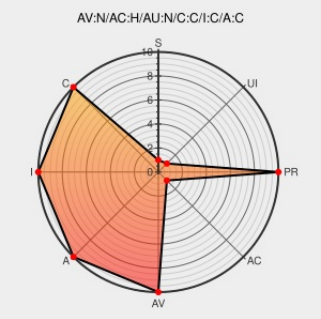
CVE-2010-4701

Published on: 01/20/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:01 PM UTC

CVE-2010-4701

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



Certain versions of Windows 2003 Server from Microsoft contain the following vulnerability:

Heap-based buffer overflow in the CDrawPoly::Serialize function in fxscover.exe in Microsoft Windows Fax Services Cover Page Editor 5.2 r2 in Windows XP Professional SP3, Server 2003 R2 Enterprise Edition SP2, and Windows 7 Professional allows remote attackers to execute arbitrary code via a long record in a Fax Cover Page (.cov) file. NOTE: some of these details are obtained from third party information.

CVE-2010-4701 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.6 - HIGH

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

CVE References

Description	Tags	Link
Microsoft Windows Fax Cover Page Editor Buffer Overflow Vulnerability - Advisories - Community	Vendor Advisory, web.archive.org, text/html	SECUNIA 42747
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:12689
Microsoft Windows Fax Services Cover Page Editor (.cov) Memory Corruption	Exploit, www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 15839
US-CERT Technical Cyber Security Alert TA11-102A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource, www.us-cert.gov	CERT TA11-102A

	text/xml	
Error 404 :(	Exploit retrogod.altervista.org text/plain Inactive Link Not Archived	MISC retrogod.altervista.org/9sg_cov_bof.html
Microsoft Fax Cover Page Editor Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1024925

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2003 Server	All	r2_sp2	enterprise	All
Operating System	Microsoft	Windows 2003 Server	All	r2_sp2	enterprise	All
Operating System	Microsoft	Windows 7	All	All	professional	All
Operating System	Microsoft	Windows 7	All	All	professional	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

cpe:2.3:o:microsoft:windows_2003_server:*:r2_sp2:enterprise:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:*:r2_sp2:enterprise:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:*:*:professional:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:*:*:professional:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report