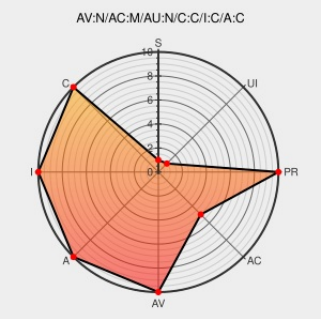
# CVE-2010-3227

Published on: 10/26/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

## CVE-2010-3227

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




Certain versions of Windows 7 from Microsoft contain the following vulnerability:

Stack-based buffer overflow in the UpdateFrameTitleForDocument method in the CFrameWnd class in mfc42.dll in the Microsoft Foundation Class (MFC) Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows context-dependent attackers to execute arbitrary code via a long window title that this library attempts to create at the request of an application, as demonstrated by the Trident PowerZip 7.2 Build 4010 application, aka "Windows MFC Document Title Updating Buffer Overflow Vulnerability."

CVE-2010-3227 has been assigned by secure@microsoft.com to track the vulnerability

### CVSS2 Score: 9.3 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| SecurityTracker.com Archives - Microsoft Foundation Classes Library Buffer Overflow in Window Title Lets Remote Users Execute Arbitrary Code | Third Party Advisory, VDB Entry, www.securitytracker.com, text/html | SECTRACK 1024557 |
| Repository / Oval Repository | Third Party Advisory, oval.cisecurity.org, text/html | OVAL oval:org.mitre.oval:def:6696 |

| | | |
|---|---|---|
| PowerZip 7.21 (Build 4010) Stack Buffer Overflow | Exploit<br>Third Party Advisory<br>VDB Entry<br>www.exploit-db.com<br>Proof of Concept<br>text/html | EXPLOIT-DB 13921 |
| Microsoft Security Bulletin MS10-074 - Moderate \| Microsoft Docs | docs.microsoft.com<br>text/html | MS MS10-074 |
| Security Webinars, Podcasts, Success Stories, White Papers, and Datasheets \| eEye Digital Security | www.eeye.com<br>text/html | MISC<br>www.eeye.com/Resources/Security-Center/Research/Zero-Day-Tracker/2010/20100705-(1) |



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 7 | All | All | All | All |
| Operating System | Microsoft | Windows 7 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2003 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Server 2003 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | - | r2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | - | r2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Vista | - | sp1 | All | All |
| Operating System | Microsoft | Windows Vista | - | sp2 | All | All |
| Operating System | Microsoft | Windows Vista | - | sp1 | All | All |
| Operating System | Microsoft | Windows Vista | - | sp2 | All | All |
| Operating System | Microsoft | Windows Xp | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Microsoft | Windows Xp | sp3 | All | All | All |
| Operating System | Microsoft | Windows Xp | - | All | All | All |
| Operating System | Microsoft | Windows Xp | sp3 | All | All | All |

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

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

cpe:2.3:o:microsoft:windows_server_2003:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:r2:*:*:*:*:x64:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:r2:*:*:*:*:x64:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:*:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:-:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→