

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search

View CVE

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Vulnerability Feeds & Widgets](#)^{New}

www.itsecdb.com

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score](#)

[Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft](#)

[References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

[Feedback](#)

[CVE Help](#)

[FAQ](#)

[Articles](#)

External Links :

[NVD Website](#)

[CWE Web Site](#)

View CVE :

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

(e.g.: 12345)

Search By Microsoft

Reference ID:

(e.g.: ms10-001 or 979352)

Vulnerability Details : [CVE-2015-2509](#)

Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted Media Center link (mcl) file, aka "Windows Media Center RCE Vulnerability."

Publish Date : 2015-09-08 Last Update Date : 2015-09-09



Gmail for Work

利用來自 Google Apps 的自訂電子郵件，讓電子郵件看起來更專業

[開始免費試用](#)

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

| | |
|------------------------|---|
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code |
| CWE ID | 20 |



Code Encryption Software

Build Secure Apps Free
Software Protection
Whitepaper

www.arxan.com/attack

- Products Affected By CVE-2015-2509

| # | Product Type | Vendor | Product | Version | Update | Edition | Language | |
|---|--------------|---------------------------|-------------------------------------|---------|--------|-----------|----------|---|
| 1 | OS | Microsoft | Windows 7 | - | SP1 | ~~~~~x86~ | | Version Details Vulnerabilities |
| 2 | OS | Microsoft | Windows 7 | - | SP1 | ~~~~~x64~ | | Version Details Vulnerabilities |
| 3 | OS | Microsoft | Windows 8 | - | | ~~~~~x64~ | | Version Details Vulnerabilities |
| 4 | OS | Microsoft | Windows 8 | - | | ~~~~~x86~ | | Version Details Vulnerabilities |
| 5 | OS | Microsoft | Windows 8.1 | - | - | ~~~~~x64~ | | Version Details Vulnerabilities |
| 6 | OS | Microsoft | Windows 8.1 | - | - | ~~~~~x86~ | | Version Details Vulnerabilities |
| 7 | OS | Microsoft | Windows Server 2008 | | SP2 | | | Version Details Vulnerabilities |
| 8 | OS | Microsoft | Windows Server 2008 | R2 | SP1 | | | Version Details Vulnerabilities |
| 9 | OS | Microsoft | Windows Vista | - | SP2 | | | Version Details Vulnerabilities |

- Number Of Affected Versions By Product

| Vendor | Product | Vulnerable Versions |
|---------------------------|-------------------------------------|---------------------|
| Microsoft | Windows 7 | 2 |
| Microsoft | Windows 8 | 2 |
| Microsoft | Windows 8.1 | 2 |
| Microsoft | Windows Server 2008 | 2 |
| Microsoft | Windows Vista | 1 |

- References For CVE-2015-2509

<http://technet.microsoft.com/en-us/security/bulletin/ms15-100>

Microsoft Security Bulletin MS15-100

+ Metasploit Modules Related To CVE-2015-2509

[How does it work? Known limitations & technical details](#) [User agreement, disclaimer and privacy statement](#) [About & Contact](#) [Feedback](#)

CVE is a registered trademark of the MITRE Corporation and the authoritative source of CVE content is [MITRE's CVE web site](#). CWE is a registered trademark of the MITRE Corporation and the authoritative source of CWE content is [MITRE's CWE web site](#). OVAL is a registered trademark of The MITRE Corporation and the

authoritative source of OVAL content is [MITRE's OVAL web site](#).

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.