



CVE-2011-1280

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2011-1280
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-16 20:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The XML Editor in Microsoft InfoPath 2007 SP2 and 2010; SQL Server 2005 SP3 and SP4 and 2008 SP1, SP2, and R2; S...

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office Infopath	2007	sp2	All	All

Application	Microsoft	Office Infopath	2010	All	x32	All
Application	Microsoft	Office Infopath	2010	All	x64	All
Application	Microsoft	Sql Server	2005	sp3	All	All
Application	Microsoft	Sql Server	2005	sp3	express	All
Application	Microsoft	Sql Server	2005	sp3	express_advanced_services	All
Application	Microsoft	Sql Server	2005	sp3	itanium	All
Application	Microsoft	Sql Server	2005	sp3	x64	All
Application	Microsoft	Sql Server	2005	sp4	All	All
Application	Microsoft	Sql Server	2005	sp4	express	All
Application	Microsoft	Sql Server	2005	sp4	express_advanced_services	All
Application	Microsoft	Sql Server	2005	sp4	itanium	All
Application	Microsoft	Sql Server	2005	sp4	x64	All
Application	Microsoft	Sql Server	2008	r2	itanium	All
Application	Microsoft	Sql Server	2008	r2	x64	All
Application	Microsoft	Sql Server	2008	sp1	itanium	All
Application	Microsoft	Sql Server	2008	sp1	x64	All
Application	Microsoft	Sql Server	2008	sp2	itanium	All
Application	Microsoft	Sql Server	2008	sp2	x32	All
Application	Microsoft	Sql Server	2008	sp2	x64	All
Application	Microsoft	Sql Server Management Studio Express	2005	All	All	All
Application	Microsoft	Sql Server Management Studio Express	2005	All	x64	All
Application	Microsoft	Visual Studio	2005	sp1	All	All
Application	Microsoft	Visual Studio	2008	sp1	All	All
Application	Microsoft	Visual Studio	2010	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
Microsoft Office InfoPath XML Editor External Entity Resolution Flaw Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrack
Repository / Oval Repository
Microsoft Visual Studio XML Editor External Entity Resolution Flaw Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrack
Microsoft SQL Server XML Editor External Entity Resolution Flaw Lets Remote Users Obtain Potentially Sensitive Information - SecurityTrack
Microsoft Security Bulletin MS11-049 - Important Microsoft Docs
Microsoft XML External Entity Resolution CVE-2011-1290 Information Disclosure Vulnerability

Microsoft AML External Entities Resolution CVE-2011-1280 Information Disclosure vulnerability

About Secunia Research | Flexera

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)