



CVE-2011-0092

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-0092
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-10 16:00:00 UTC
Updated	2018-10-12 21:59:00 UTC
Description	The LZW stream decompression functionality in ORMELEMS.DLL in Microsoft Visio 2002 SP2, 2003 SP3, and 2007 SP2 a

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visio	2002	sp2	All	All
Application	Microsoft	Visio	2003	sp3	All	All
Application	Microsoft	Visio	2007	sp2	All	All
Application	Microsoft	Visio	2002	sp2	All	All
Application	Microsoft	Visio	2003	sp3	All	All
Application	Microsoft	Visio	2007	sp2	All	All

References

Reference	Source
Microsoft Security Bulletin MS11-008 - Important Microsoft Docs	MS
SecurityFocus	BUGTRAQ
70828	OSVDB
Microsoft Visio Object Memory Corruption (CVE-2011-0092) Remote Code Execution Vulnerability	BID
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Repository / Oval Repository	OVAL
Microsoft Visio Memory Corruption Error in Processing Visio Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRAC

Zero Day Initiative	MISC
Microsoft Visio Two Memory Corruption Vulnerabilities - Secunia.com	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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](#)