



CVE-2006-0009

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

Summary

CVE	CVE-2006-0009
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-14 23:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in Microsoft Office 2000 SP3, XP SP3, and other versions and packages, allows user-assisted attackers to

Risk And Classification

Primary CVSS: v2.0 5.1 from nvd@nist.gov

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

EPSS: 0.413870000 probability, percentile 0.974080000 (date 2026-04-17)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Microsoft	Office	2000	sp3	All	All
Application	Microsoft	Office	2003	sp1	All	All
Application	Microsoft	Office	2003	sp2	All	All
Application	Microsoft	Office	2004	All	mac	All
Application	Microsoft	Office	v.x	All	mac	All
Application	Microsoft	Office	xp	sp3	All	All
Application	Microsoft	Works	2000	All	All	All
Application	Microsoft	Works	2001	All	All	All
Application	Microsoft	Works	2002	All	All	All
Application	Microsoft	Works	2003	All	All	All
Application	Microsoft	Works	2004	All	All	All
Application	Microsoft	Works	2005	All	All	All
Application	Microsoft	Works	2006	All	All	All

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

References	
Reference	Source
symantec.com has moved to broadcom.com	af854
SecurityFocus	af854
Repository / Oval Repository	af854
Retired: Microsoft PowerPoint Remote Code Execution Vulnerability	af854
SecuriTeam Blogs » Juha-Matti	af854
Repository / Oval Repository	af854
SecurityFocus	af854
Trojan.PPDropper.E - Symantec.com	af854
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
SecurityFocus	af854
SecurityFocus	af854
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
IBM X-Force Exchange	af854
1. Overview:	af854
SecurityTracker.com Archives - Microsoft Office and Excel Buffer Overflows Let Remote Users Execute Arbitrary Code	af854
SecurityTracker.com Archives - [Duplicate] Microsoft PowerPoint Bug Lets Remote Users Execute Arbitrary Code	af854

NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854
[Full-disclosure] Yet another 0day for IE	af854
TROJ_MDROPPE.BH - Description and solution	af854
Repository / Oval Repository	af854
Microsoft Security Bulletin MS06-012 - Critical Microsoft Docs	af854
401 Authorization Required	af854
Microsoft Office Multiple Code Execution Vulnerabilities - Advisories - Secunia	af854
SecurityFocus	af854
Microsoft Office Routing Slip Processing Remote Buffer Overflow Vulnerability	af854
www.osvdb.org/23903	af854
SecurityFocus	af854
Repository / Oval Repository	af854
SecuriTeam Blogs » New PowerPoint 0-day and related Trojan in the wild	af854
SANS - Internet Storm Center - Cooperative Cyber Threat Monitor And Alert System	af854
US-CERT Technical Cyber Security Alert TA06-073A -- Microsoft Office and Excel Vulnerabilities	af854
IBM X-Force Exchange	af854
SecurityTracker.com Archives - [Duplicate Entry] Microsoft PowerPoint Unknown Bug May Let Remote Users Execute Arbitrary Code	af854
Avaya Modular Messaging Windows Privilege Escalation Security Issues - Advisories - Secunia	af854
US-CERT Vulnerability Note VU#682820	af854
www.darkreading.com/document.asp	af854
TROJ_MDROPPE.BH - Description and solution	MITR
CVE Program record	CVE.
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](#)