



CVE-2006-0029

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

Summary

CVE	CVE-2006-0029
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	Unspecified vulnerability in Microsoft Excel 2000, 2002, and 2003, in Microsoft Office 2000 SP3 and other packages, allows

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: 0.253650000 probability, percentile 0.962180000 (date 2026-04-17)

Problem Types: NVD-CWE-noinfo | 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	Excel	2000	All	All	All
Application	Microsoft	Excel	2002	All	All	All
Application	Microsoft	Excel	2003	All	All	All
Application	Microsoft	Excel	2004	All	mac_os_x	All
Application	Microsoft	Excel	x	All	mac_os_x	All
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

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

References	
Reference	Source
IBM X-Force Exchange	af854a3a-2127-422b-b000-000000000000
Repository / Oval Repository	af854a3a-2127-422b-b000-000000000000
US-CERT Vulnerability Note VU#235774	af854a3a-2127-422b-b000-000000000000
www.osvdb.org/23900	af854a3a-2127-422b-b000-000000000000
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-b000-000000000000
1. Overview:	af854a3a-2127-422b-b000-000000000000
Repository / Oval Repository	af854a3a-2127-422b-b000-000000000000
SecurityTracker.com Archives - Microsoft Office and Excel Buffer Overflows Let Remote Users Execute Arbitrary Code	af854a3a-2127-422b-b000-000000000000
SecurityReason	af854a3a-2127-422b-b000-000000000000
Microsoft Security Bulletin MS06-012 - Critical Microsoft Docs	af854a3a-2127-422b-b000-000000000000
Microsoft Office Multiple Code Execution Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-b000-000000000000
Repository / Oval Repository	af854a3a-2127-422b-b000-000000000000
SecurityReason	af854a3a-2127-422b-b000-000000000000
US-CERT Technical Cyber Security Alert TA06-073A -- Microsoft Office and Excel Vulnerabilities	af854a3a-2127-422b-b000-000000000000
Repository / Oval Repository	af854a3a-2127-422b-b000-000000000000
Avaya Modular Messaging Windows Privilege Escalation Security Issues - Advisories - Secunia	af854a3a-2127-422b-b000-000000000000
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](#)