CVE-2007-0208

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

Summary

CVE	CVE-2007-0208
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-13 21:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Microsoft Word in Office 2000 SP3, XP SP3, Office 2003 SP2, Works Suite 2004 to 2006, and Office 2004 for Mac does no

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

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	sp2	All	All
Application	Microsoft	Office	2004	All	mac	All
Application	Microsoft	Office	xp	sp3	All	All
Application	Microsoft	Word	2000	All	All	All
Application	Microsoft	Word	2002	All	All	All
Application	Microsoft	Word	2003	All	All	All
Application	Microsoft	Word Viewer	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
Repository / Oval Repository
Microsoft Word Macro Permissions Bypass Arbitrary Code Execution Vulnerability
Microsoft Word Macro Security Warning Bug and Drawing Object Memory Corrupution Error Lets Remote Users Execute Arbitrary Code - Sec
Microsoft Security Bulletin MS07-014 - Critical | Microsoft Docs
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.osvdb.org/34385
US-CERT Technical Cyber Security Alert TA07-044A -- Microsoft Updates for Multiple Vulnerabilities
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**