CVE-2003-0664

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

Summary

CVE	CVE-2003-0664
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-10-20 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Microsoft Word 2002, 2000, 97, and 98(J) does not properly check certain properties of a document, which allows attackers

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Word	2000	All	All	All

Application	Microsoft	Word	2000	sp2	All	All
Application	Microsoft	Word	2000	sp3	All	All
Application	Microsoft	Word	2000	sr1	All	All
Application	Microsoft	Word	2000	sr1a	All	All
Application	Microsoft	Word	2002	All	All	All
Application	Microsoft	Word	2002	sp1	All	All
Application	Microsoft	Word	2002	sp2	All	All
Application	Microsoft	Word	97	All	All	All
Application	Microsoft	Word	97	sr1	All	All
Application	Microsoft	Word	97	sr2	All	All
Application	Microsoft	Word	98	All	All	All
Application	Microsoft	Word	98	All	All	ja
Application	Microsoft	Works	2001	All	All	All
Application	Microsoft	Works	2002	All	All	All
Application	Microsoft	Works	2003	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
Microsoft Security Bulletin MS03-035 - Important | Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108	docs.microsoft.com	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org	Third
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

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**