# CVE-2006-2492

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2006-2492 |
| **State** | PUBLISHED |
| **Assigner** | certcc |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2006-05-20 00:02:00 UTC |
| **Updated** | 2026-04-16 14:02:14 UTC |
| **Description** | Buffer overflow in Microsoft Word in Office 2000 SP3, Office XP SP3, Office 2003 Sp1 and SP2, and Microsoft Works Suite |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.740840000 probability, percentile 0.988510000 (date 2026-05-04)

**CISA KEV:** Listed on 2022-06-08; due 2022-06-22; ransomware use Unknown

**Problem Types:** CWE-120 | n/a | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 7.6 | | AV:N/AC:H/Au:N/C:C/I:C/A:C |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | Microsoft |
| **Product** | Word |
| **Name** | Microsoft Word Malformed Object Pointer Vulnerability |
| **Required Action** | Apply updates per vendor instructions. |
| **Notes** | https://nvd.nist.gov/vuln/detail/CVE-2006-2492 |

## 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 | xp | sp3 | All | All |
| Application | Microsoft | Works Suite | All | All | All | All |

## Vendor Declared Affected Products

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

## References

| Reference |
|---|
| Microsoft Word Malformed Object Pointer Remote Code Execution Vulnerability |
| Microsoft Security Advisory (919637): Vulnerability in Word Could Allow Remote Code Execution |
| www.osvdb.org/25635 |
| Microsoft Word Malformed Object Pointer Vulnerability - Advisories - Secunia |
| Repository / Oval Repository |
| Repository / Oval Repository |
| SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc |
| SecurityTracker.com Archives - Microsoft Word Lets Remote Users Cause Arbitrary Code to Be Executed |
| US-CERT Vulnerability Note VU#446012 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| SANS Internet Storm Center; Cooperative Network Security Community - Internet Security - isc |
| Welcome to the Microsoft Security Response Center Blog! : Reports of a new vulnerability in Microsoft Word |
| US-CERT Technical Cyber Security Alert TA06-139A -- Microsoft Word Vulnerability |
| Microsoft Security Bulletin MS06-027 - Critical \| Microsoft Docs |
| www.cisa.gov/known-exploited-vulnerabilities-catalog |
| IBM X-Force Exchange |
| US-CERT Technical Cyber Security Alert TA06-164A -- Microsoft Windows, Internet Explorer, Media Player, Word, PowerPoint, and Exchange |
| Repository / Oval Repository |
| CVE Program record |
| NVD vulnerability detail |
| CISA Known Exploited Vulnerabilities catalog |

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| ADP | 2022-06-08T00:00:00.000Z | CVE-2006-2492 added to CISA KEV |

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**