



# CVE-2004-0210

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-0210
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-08-06 04:00:00 UTC
<b>Updated</b>	2019-04-30 14:27:00 UTC
<b>Description</b>	The POSIX component of Microsoft Windows NT and Windows 2000 allows local users to execute arbitrary code via certain

## Risk And Classification

**EPSS:** 0.051160000 probability, percentile 0.898060000 (date 2026-04-01)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** NVD-CWE-Other

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Windows
<b>Name</b>	Microsoft Windows Privilege Escalation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2004-0210">https://nvd.nist.gov/vuln/detail/CVE-2004-0210</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Avaya</a>	<a href="#">Modular Messaging Message Storage Server</a>	s3400	All	All	All
Operating System	<a href="#">Avaya</a>	<a href="#">Modular Messaging Message Storage Server</a>	s3400	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp2	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp3	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp4	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp2	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp3	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 2000</a>	All	sp4	All	All

Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6	alpha	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6	terminal_server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	enterprise_server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	workstation	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6	alpha	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6	terminal_server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	enterprise_server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	server	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Nt</a>	4.0	sp6a	workstation	All

## References

Reference	Source
Repository / Oval Repository	OV
Repository / Oval Repository	OV
US-CERT Technical Cyber Security Alert TA04-196A -- Multiple Vulnerabilities in Microsoft Windows Components and Outlook Express	CE
US-CERT Vulnerability Note VU#647436	CE
Microsoft Security Bulletin MS04-020 - Important   Microsoft Docs	MS
IBM X-Force Exchange	XF
CVE Program record	CV
NVD vulnerability detail	NV
CISA Known Exploited Vulnerabilities catalog	CIS

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)