



CVE-2006-2370

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

Summary

CVE	CVE-2006-2370
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-13 19:06:00 UTC
Updated	2019-04-30 14:27:00 UTC
Description	Buffer overflow in the Routing and Remote Access service (RRAS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	All	All	All

Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2		All	datacenter_64-bit
Operating System	Microsoft	Windows 2003 Server	sp1		All	enterprise
Operating System	Microsoft	Windows 2003 Server	standard		All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1		All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit		All	All
Operating System	Microsoft	Windows 2003 Server	web		All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1		All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition		All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1		All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit		All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	sp1		All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit		All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1		All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit		All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	sp1		All
Operating System	Microsoft	Windows 2003 Server	r2		All	datacenter_64-bit
Operating System	Microsoft	Windows 2003 Server	sp1		All	enterprise
Operating System	Microsoft	Windows 2003 Server	standard		All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1		All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit		All	All
Operating System	Microsoft	Windows 2003 Server	web		All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1		All
Operating System	Microsoft	Windows Xp	All		All	64-bit
Operating System	Microsoft	Windows Xp	All		All	home
Operating System	Microsoft	Windows Xp	All		All	media_center
Operating System	Microsoft	Windows Xp	All		gold	professional
Operating System	Microsoft	Windows Xp	All		sp1	home
Operating System	Microsoft	Windows Xp	All		sp1	media_center
Operating System	Microsoft	Windows Xp	All		sp2	home
Operating System	Microsoft	Windows Xp	All		sp2	media_center
Operating System	Microsoft	Windows Xp	All		sp2	tablet_pc
Operating System	Microsoft	Windows Xp	All		All	64-bit
Operating System	Microsoft	Windows Xp	All		All	home
Operating System	Microsoft	Windows Xp	All		All	media_center

Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

References

Reference

Repository / Oval Repository

26437

IBM X-Force Exchange

Repository / Oval Repository

Secunia - Advisories - Microsoft Windows Routing and Remote Access Vulnerabilities

Repository / Oval Repository

Microsoft Security Bulletin MS06-025 - Critical | Microsoft Docs

Microsoft Windows Routing and Remote Access Remote Code Execution Vulnerability

Repository / Oval Repository

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Repository / Oval Repository

US-CERT Technical Cyber Security Alert TA06-164A -- Microsoft Windows, Internet Explorer, Media Player, Word, PowerPoint, and Exchange

Repository / Oval Repository

SecurityTracker.com Archives - Windows Routing and Remote Access Service RPC Buffer Overflows Let Remote Users Execute Arbitrary Co

US-CERT Vulnerability Note VU#631516

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.

© 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