



CVE-2006-2373

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

Summary

CVE	CVE-2006-2373
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-13 19:06:00 UTC
Updated	2019-03-26 19:17:00 UTC
Description	The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows Server 2003	-	-	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	-	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Xp	-	-	All	All
Operating System	Microsoft	Windows Xp	-	sp1	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	-	All	All
Operating System	Microsoft	Windows Xp	-	sp1	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All

References

Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Microsoft Security Bulletin MS06-030 - Critical Microsoft Docs
26440
Secunia - Advisories - Windows SMB Denial of Service and Privilege Escalation
Repository / Oval Repository
Accenture Let there be change
Repository / Oval Repository
Repository / Oval Repository
Microsoft Windows SMB Driver Local Privilege Escalation Vulnerability
IBM X-Force Exchange
Repository / Oval Repository
SecurityTracker.com Archives - Windows Server Message Block Processing Bugs Let Local Users Gain Elevated Privileges or Deny Service
Repository / Oval Repository
Repository / Oval Repository
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