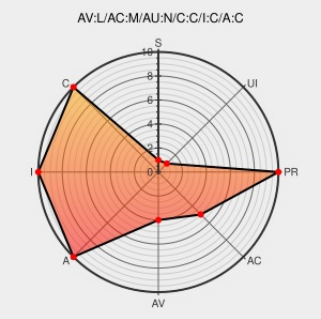
CVE-2009-1922

Published on: 08/12/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

CVE-2009-1922

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

The Message Queuing (aka MSMQ) service for Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP2, and Vista Gold does not properly validate unspecified IOCTL request data from user mode before passing this data to kernel mode, which allows local users to gain privileges via a crafted request, aka "MSMQ Null Pointer Vulnerability."

CVE-2009-1922 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Vulnerabilities	web.archive.org text/html Inactive Link Not Archived	MISC en.securitylab.ru/lab/PT-2008-09
Microsoft Windows Message Queuing Service Privilege Escalation - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 36214
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 56901
Microsoft Security Bulletin MS09-040 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS09-040

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6109
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20090812 [PT-2008-09] Microsoft Windows MSMQ Privilege Escalation Vulnerability
US-CERT Technical Cyber Security Alert TA09-223A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	CERT TA09-223A
SecurityTracker.com Archives - Windows Message Queuing Service (MSMQ) NULL Pointer Flaw Lets Local Users Gain Elevated Privileges	www.securitytracker.com text/html	SECTRACK 1022714

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	-	-	x64	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Vista	-	-	x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:-:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:-:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→