CVE-2012-0005

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

Summary

CVE	CVE-2012-0005
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-10 21:55:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Ser

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 Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

References

Reference	Source
Windows Client-Server Run-time Subsystem Unicode Processing Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTR
US-CERT Alert TA12-010A - Microsoft Updates for Multiple Vulnerabilities	CERT
Security Alerts - Secunia	SECUN
Microsoft Windows CSRSS CVE-2012-0005 Local Privilege Escalation Vulnerability	BID
Microsoft Security Bulletin MS12-003 - Important | Microsoft Docs	MS
Repository / Oval Repository	OVAL
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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**