CVE-2007-5352

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

Summary

CVE	CVE-2007-5352
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-08 20:46:00 UTC
Updated	2018-10-15 21:43:00 UTC
Description	Unspecified vulnerability in Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2,

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	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All

References

Reference	Source	Link
US-CERT Technical Cyber Security Alert TA08-008A -- Microsoft Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov
Microsoft Security Bulletin MS08-002 - Important | Microsoft Docs	MS	docs.microsoft.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcl
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
SecurityTracker.com Archives - Microsoft Windows LSASS Lets Local Users Gain Elevated Privileges	SECTRACK	securitytracker.com
Repository / Oval Repository	OVAL	oval.cisecurity.org

US-CERT Vulnerability Note VU#410025	CERT-VN	www.kb.cert.org
Microsoft Windows LSASS Privilege Escalation Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Microsoft Windows LSASS LPC Request Local Privilege Escalation Vulnerability	BID	www.securityfocus.cor
SecurityFocus	HP	www.securityfocus.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.