CVE-2008-5416

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

Summary

CVE	CVE-2008-5416
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-10 14:00:00 UTC
Updated	2018-10-12 21:49:00 UTC
Description	Heap-based buffer overflow in Microsoft SQL Server 2000 SP4, 8.00.2050, 8.00.2039, and earlier; SQL Server 2000 Deskt

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Sql Server	2000	All	All	All
Application	Microsoft	Sql Server	2005	All	All	All
Application	Microsoft	Sql Server	2000	All	All	All
Application	Microsoft	Sql Server	2005	All	All	All

References

Reference	Sou
Microsoft Security Bulletin MS09-004 - Important | Microsoft Docs	MS
IBM X-Force Exchange	XF
Microsoft SQL Server sp_replwritetovarbin() Heap Overflow Exploit	EXP
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FUL
SecurityFocus	BUG
US-CERT Vulnerability Note VU#696644	CER
VMSA-2011-0003	CON
SecurityTracker.com Archives - Microsoft SQL Server Heap Overflow Lets Remote Authenticated Users Execute Arbitrary Code	SEC
SecurityFocus	BUG
CXSecurity - IDS	SRE

50917	OSV
Microsoft SQL Server Memory Overwrite Bug in sp_replwritetovarbin May Let Remote Users Execute Arbitrary Code - SecurityTracker	SEC
Repository / Oval Repository	OVA
Your request has been blocked. This could be due to several reasons.	CON
ASA-2009-055 (959420)	CON
Microsoft SQL Server "sp_replwritetovarbin()" Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUP
US-CERT Technical Cyber Security Alert TA09-041A -- Microsoft Updates for Multiple Vulnerabilities	CER
SecurityFocus	BUG
VMware vCenter Server 4.1 Update 1 Release Notes	CON
404 - Page not found! - SEC Consult	MIS
Microsoft SQL Server 'sp_replwritetovarbin' Remote Memory Corruption Vulnerability	BID
CVE Program record	CVE
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**