CVE-2006-3590

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

Summary

CVE	CVE-2006-3590
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-14 18:05:00 UTC
Updated	2018-10-18 16:48:00 UTC
Description	mso.dll, as used by Microsoft PowerPoint 2000 through 2003, allows user-assisted attackers to execute arbitrary command

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Powerpoint	2000	All	All	All
Application	Microsoft	Powerpoint	2002	All	All	All
Application	Microsoft	Powerpoint	2003	All	All	All
Application	Microsoft	Powerpoint	2003	sp1	All	All
Application	Microsoft	Powerpoint	2003	sp2	All	All
Application	Microsoft	Powerpoint	2000	All	All	All
Application	Microsoft	Powerpoint	2002	All	All	All
Application	Microsoft	Powerpoint	2003	All	All	All
Application	Microsoft	Powerpoint	2003	sp1	All	All
Application	Microsoft	Powerpoint	2003	sp2	All	All

References

Reference	Source
Microsoft Powerpoint Remote Code Execution Vulnerability	BID
Trojan.PPDropper.B - Symantec.com	MISC
SecurityFocus	BUGTRAQ
Microsoft PowerPoint Code Execution Vulnerabilities - Advisories - Secunia	SECUNIA

27324	OSVDB
US-CERT Technical Cyber Security Alert TA06-220A -- Microsoft Products Contain Multiple Vulnerabilities	CERT
InfoSec Handlers Diary Blog	MISC
IBM X-Force Exchange	XF
IBM X-Force Exchange	XF
SecurityTracker.com Archives - Microsoft PowerPoint 'mso.dll' Buffer Overflow May Let Remote Users Execute Arbitrary Code	SECTRACK
SecurityFocus	BUGTRAQ
Microsoft Security Bulletin MS06-048 - Critical | Microsoft Docs	MS
Repository / Oval Repository	OVAL
US-CERT Vulnerability Note VU#936945	CERT-VN
SecuriTeam Blogs » Microsoft PowerPoint 0-day Vulnerability FAQ [UPDATED]	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityFocus	BUGTRAQ
CVE Program record	CVE.ORG
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**