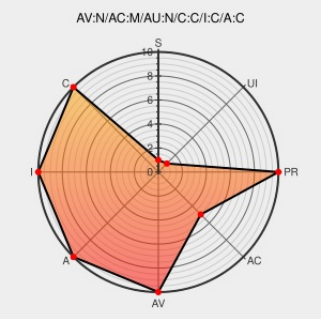
CVE-2006-1540

Published on: 03/30/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1540

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



Certain versions of Office from Microsoft contain the following vulnerability:

MSO.DLL in Microsoft Office 2000, Office XP (2002), and Office 2003 allows user-assisted attackers to cause a denial of service and execute arbitrary code via multiple attack vectors, as originally demonstrated using a crafted document record with a malformed string, as demonstrated by replacing a certain "01 00 00 00" byte sequence with an "FF FF FF FF" byte sequence, possibly causing an invalid array index, in (1) an Excel .xls document, which triggers an access violation in ole32.dll; (2) an Excel .xlw document, which triggers an access violation in excel.exe; (3) a Word document, which triggers an access violation in mso.dll in winword.exe; and (4) a PowerPoint document, which triggers an access violation in powerpnt.txt. NOTE: after the initial disclosure, this issue was demonstrated by triggering an integer overflow using an inconsistent size for a Unicode "Sheet Name" string.

CVE-2006-1540 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Microsoft Office Products - Array Index Bounds Error (PoC) - Windows dos Exploit	Third Party Advisory, VDB Entry, www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 1615

US-CERT Technical Cyber Security Alert TA06-192A -- Microsoft Windows, Office, and IIS Vulnerabilities	Third Party Advisory US Government Resource www.us-cert.gov text/html	CERT TA06-192A
Microsoft Office Malformed String Parsing Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 18889
SecurityTracker.com Archives - Microsoft Office Array Index Boundary Error Lets Remote Users Execute Arbitrary Code	Exploit Third Party Advisory VDB Entry securitytracker.com text/html	SECTRACK 1015855
Microsoft Office XP Array Index Denial of Service Vulnerability	Exploit Third Party Advisory VDB Entry cve.report (archive) text/html	BID 17252
US-CERT Vulnerability Note VU#609868	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#609868
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:639
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-2756
Microsoft Office String and Property Parsing Vulnerabilities - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 21012
Microsoft Security Bulletin MS06-038 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS06-038
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF office-property-string-bo(27609)
No Description Provided	Broken Link www.osvdb.org Inactive Link Not Archived	OSVDB 27150
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF office-string-parse-bo(27607)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060710 SYMSA-2006-007: Microsoft Office Malformed String Parsing Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	All	All	All	All
Application	Microsoft	Office	2000	All	All	All
Application	Microsoft	Office	2000	All	All	ja
Application	Microsoft	Office	2000	All	All	ko
Application	Microsoft	Office	2000	All	All	zh
Application	Microsoft	Office	2000	sp1	All	All
Application	Microsoft	Office	2000	sp3	All	All
Application	Microsoft	Office	2003	All	All	All
Application	Microsoft	Office	2003	sp1	All	All
Application	Microsoft	Office	2003	sp2	All	All
Application	Microsoft	Office	2004	All	All	All
Application	Microsoft	Office	v.x	All	All	All
Application	Microsoft	Office	xp	sp1	All	All
Application	Microsoft	Office	xp	sp2	All	All
Application	Microsoft	Office	xp	sp3	All	All
Application	Microsoft	Office	All	All	All	All
Application	Microsoft	Office	2000	All	All	All
Application	Microsoft	Office	2000	All	All	ja
Application	Microsoft	Office	2000	All	All	ko
Application	Microsoft	Office	2000	All	All	zh
Application	Microsoft	Office	2000	sp1	All	All
Application	Microsoft	Office	2000	sp3	All	All
Application	Microsoft	Office	2003	All	All	All
Application	Microsoft	Office	2003	sp1	All	All
Application	Microsoft	Office	2003	sp2	All	All
Application	Microsoft	Office	2004	All	All	All
Application	Microsoft	Office	v.x	All	All	All
Application	Microsoft	Office	xp	sp1	All	All
Application	Microsoft	Office	xp	sp2	All	All
Application	Microsoft	Office	xp	sp3	All	All

cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:ja:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:ko:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:zh:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2003:*:*:*:student_teacher:*:*:*:

cpe:2.3:a:microsoft:office:2003:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2003:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2004:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:microsoft:office:v.x:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:microsoft:office:xp:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:xp:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:xp:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:ja:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:ko:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:*:*:zh:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2000:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2003:*:*:*:student_teacher:*:*:*:

cpe:2.3:a:microsoft:office:2003:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2003:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2004:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:microsoft:office:v.x:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:microsoft:office:xp:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:xp:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office:xp:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→