



CVE-2006-0010

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2006-0010
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-10 22:03:00 UTC
Updated	2019-04-30 14:27:00 UTC
Description	Heap-based buffer overflow in T2MBED.DLL in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to S

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All

Operating System	Microsoft	Windows 2003 Server	r2	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	enterprise	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98	All	gold	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows 98se	All	All	All	All
Operating System	Microsoft	Windows Me	All	All	All	All
Operating System	Microsoft	Windows Me	All	All	All	All
Operating System	Microsoft	Windows Nt	3.5.1	All	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp1	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp2	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp3	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp4	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp5	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp5	alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All

Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server_alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	All	All
Operating System	Microsoft	Windows Nt	4.0	sp1	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	All	All
Operating System	Microsoft	Windows Nt	4.0	sp2	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	All	All
Operating System	Microsoft	Windows Nt	4.0	sp3	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	All	All
Operating System	Microsoft	Windows Nt	4.0	sp4	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	All	All
Operating System	Microsoft	Windows Nt	4.0	sp5	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	All	All

Operating System	Microsoft	Windows Nt	4.0	sp6	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	All	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Nt	3.5.1	All	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp1	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp2	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp3	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp4	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp5	All	All
Operating System	Microsoft	Windows Nt	3.5.1	sp5	alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server_alpha	All
Operating System	Microsoft	Windows Nt	4.0	All	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp1	All	All
Operating System	Microsoft	Windows Nt	4.0	sp1	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp2	All	All
Operating System	Microsoft	Windows Nt	4.0	sp2	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All

Operating System	Microsoft	Windows Nt	4.0	sp2	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp3	All	All
Operating System	Microsoft	Windows Nt	4.0	sp3	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp4	All	All
Operating System	Microsoft	Windows Nt	4.0	sp4	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp5	All	All
Operating System	Microsoft	Windows Nt	4.0	sp5	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	All	All
Operating System	Microsoft	Windows Nt	4.0	sp6	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	All	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	alpha	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All

Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

References

Reference	Source
Secunia - Advisories - Avaya Products Microsoft Windows Embedded Web Fonts Code Execution	SEC
Repository / Oval Repository	OVA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
Microsoft Security Bulletin MS06-002 - Critical Microsoft Docs	MS
Repository / Oval Repository	OVA
SecurityTracker.com Archives - Microsoft Windows Embedded Web Fonts Buffer Overflow Lets Remote Users Execute Arbitrary Code	SEC
Repository / Oval Repository	OVA
18829	OSV
Full Disclosure: [EEYEB-2000801] - Windows Embedded Open Type (EOT) Font Heap Overflow Vulnerability	FUL
Secunia - Advisories - Microsoft Windows Embedded Web Fonts Code Execution Vulnerability	SEC
IBM X-Force Exchange	XF
Repository / Oval Repository	OVA
Nortel: Technical Support	MIS
Nortel Centrex IP Client Manager Multiple Vulnerabilities - Advisories - Secunia	SEC
Repository / Oval Repository	OVA
Repository / Oval Repository	OVA
Microsoft Windows Embedded Web Font Buffer Overflow Vulnerability	BID
US-CERT Vulnerability Note VU#915930	CEF
US-CERT Technical Cyber Security Alert TA06-010A -- Microsoft Windows, Outlook, and Exchange Vulnerabilities	CEF

SecurityFocus	BUG
support.avaya.com/elmodocs2/security/ASA-2006-004.htm	CON
BeyondTrust Privileged Access Management, Cyber Security, and Remote Access (formerly Bomgar) BeyondTrust	EEY
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)