



CVE-2006-4662

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

Summary

CVE	CVE-2006-4662
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-09 00:04:00 UTC
Updated	2018-10-17 21:38:00 UTC
Description	Heap-based buffer overflow in the MCRexEx__Search function in AOL ICQ Pro 2003b Build 3916 and earlier allows remote

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mirabilis	Icq	0.99b_1.1.1.1	All	All	All
Application	Mirabilis	Icq	0.99b_v.3.19	All	All	All
Application	Mirabilis	Icq	2000.0a	All	All	All
Application	Mirabilis	Icq	2000.0b_build3278	All	All	All
Application	Mirabilis	Icq	2001a	All	All	All
Application	Mirabilis	Icq	2001b_build3636	All	All	All
Application	Mirabilis	Icq	2001b_build3638	All	All	All
Application	Mirabilis	Icq	2001b_build3659	All	All	All
Application	Mirabilis	Icq	2002a_build3722	All	All	All
Application	Mirabilis	Icq	2002a_build3727	All	All	All
Application	Mirabilis	Icq	2003a	All	All	All
Application	Mirabilis	Icq	2003a_build3777	All	All	All
Application	Mirabilis	Icq	2003a_build3799	All	All	All
Application	Mirabilis	Icq	2003a_build3800	All	All	All
Application	Mirabilis	Icq	2003b	All	All	All
Application	Mirabilis	Icq	2003b_build3096	All	pro	All
Application	Mirabilis	Icq	98.0a	All	All	All

Application	Mirabilis	lcq	99a_2.15build1701	All	All	All
Application	Mirabilis	lcq	99a_2.21build1800	All	All	All
Application	Mirabilis	lcq	0.99b_1.1.1.1	All	All	All
Application	Mirabilis	lcq	0.99b_v.3.19	All	All	All
Application	Mirabilis	lcq	2000.0a	All	All	All
Application	Mirabilis	lcq	2000.0b_build3278	All	All	All
Application	Mirabilis	lcq	2001a	All	All	All
Application	Mirabilis	lcq	2001b_build3636	All	All	All
Application	Mirabilis	lcq	2001b_build3638	All	All	All
Application	Mirabilis	lcq	2001b_build3659	All	All	All
Application	Mirabilis	lcq	2002a_build3722	All	All	All
Application	Mirabilis	lcq	2002a_build3727	All	All	All
Application	Mirabilis	lcq	2003a	All	All	All
Application	Mirabilis	lcq	2003a_build3777	All	All	All
Application	Mirabilis	lcq	2003a_build3799	All	All	All
Application	Mirabilis	lcq	2003a_build3800	All	All	All
Application	Mirabilis	lcq	2003b	All	All	All
Application	Mirabilis	lcq	2003b_build3096	All	pro	All
Application	Mirabilis	lcq	98.0a	All	All	All
Application	Mirabilis	lcq	99a_2.15build1701	All	All	All
Application	Mirabilis	lcq	99a_2.21build1800	All	All	All

References						
Reference			Source	Link	Ta	
SecurityFocus			BUGTRAQ	www.securityfocus.com		
SecurityReason - AOL ICQ Pro 2003b heap overflow vulnerability			SREASON	securityreason.com		
ICQ Pro 2003b "MCRex__Search" Buffer Overflow Vulnerability - Advisories - Secunia			SECUNIA	secunia.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN	www.vupen.com		
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
US-CERT Vulnerability Note VU#400780			CERT-VN	www.kb.cert.org	US	
Core Security CoreLabs			MISC	www.coresecurity.com	Pa	
ICQ MCRex__Search Remote Heap Buffer Overflow Vulnerability			BID	www.securityfocus.com	Pa	
CVE Program record			CVE.ORG	www.cve.org	ca	
NVD vulnerability detail			NVD	nvd.nist.gov	ca	

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](#).

Free CVE JSON API [cve.report/api](#)

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