



CVE-2002-0425

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

Summary

CVE	CVE-2002-0425
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-08-12 04:00:00 UTC
Updated	2008-09-05 20:27:00 UTC
Description	mIRC DCC server protocol allows remote attackers to gain sensitive information such as alternate IRC nicknames via a "10

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Khaled Mardam-bey	Mirc	6.0	All	All	All
Application	Khaled Mardam-bey	Mirc	6.0_1	All	All	All
Application	Khaled Mardam-bey	Mirc	6.0	All	All	All
Application	Khaled Mardam-bey	Mirc	6.0_1	All	All	All

References

Reference
5301
ISS X-Force Database: mirc-dcc-reveal-info (8393): mIRC DCC "100 testing" command could reveal the nickname and the number of IRC ser
mIRC DCC Nick Disclosure Vulnerability
SecurityFocus HOME Mailing List: BugTraQ
CVE Program record
NVD vulnerability detail

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](#)