

# [NT] mIRC DCC Vulnerability (Long Filename)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0113.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 10/26/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 26 Oct 2003 18:48:42 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

mIRC DCC Vulnerability (Long Filename)

---

## SUMMARY

Another exploit was identified that can crash even the recently released version 6.12. It only seems to affect people who minimize DCC get dialog windows (manually or by default), and then open those windows to get a file with an excessively long filename. You cannot be crashed unless that sequence of events occurs. That manual step is required. If you auto-get the file, or do not get the file at all, nothing happens.

## DETAILS

Vulnerable systems:

- \* mIRC version 6.12

Workaround:

If you think the above affects you, then here is a temporary fix that should be pasted in your "remotes" section (alt-r to access). The below script rejects any excessively long filename:

```
ctcp *:dcc send*: if ($len($nopath($filename)) >= 225) { echo 4 -s $nick  
tried to crash you with an illegal dcc send of $nopath($filename) | halt }
```

Alternatively, this shorter version without the warning message:

```
ctcp *:dcc send*: if ($len($nopath($filename)) >= 225) halt
```

Securiteam: [NT] mIRC DCC Vulnerability (Long Filename)

If you are not comfortable with modifying your remotes, you can just ignore all incoming DCC sends with the following, which is the same temporary fix as for the other bug described in the next section:

`/ignore -wd *`

You can undo the above command by `/ignore -rwd *` (note the r for remove).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Special-Alerts@k-otik.com>>  
K-OTiK Security.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

`list-unsubscribe@securiteam.com`

In order to subscribe to the mailing list, simply forward this email to: `list-subscribe@securiteam.com`

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.