



# CVE-2004-1052

Published on: 11/18/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

## CVE-2004-1052

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Bnc](#) from [Bnc](#) contain the following vulnerability:

Buffer overflow in the getnickuserhost function in BNC 2.8.9, and possibly other versions, allows remote IRC servers to execute arbitrary code via an IRC server response that contains many (1) ! (exclamation) or (2) @ (at sign) characters.

CVE-2004-1052 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**COMPLETE**

Integrity  
Impact

**COMPLETE**

Availability  
Impact

**COMPLETE**

## CVE References

Description

Tags

Link

'BNC 2.8.9 remote buffer overflow' - MARC

[marc.info](#)  
[text/html](#)

[BUGTRAQ 20041110 BNC 2.8.9 remote buffer overflow](#)

BNC getnickuserhost IRC Server Response Buffer Overflow Vulnerability

[Patch](#)  
[Vendor Advisory](#)  
[cve.report \(archive\)](#)  
[text/html](#)

[BID 11647](#)

404 Not Found

[web.archive.org](#)  
[text/html](#)  
[Inactive Link](#) [Not Archived](#)

[MISC security.lss.hr/en/index.php?page=details&ID=LSS-2004-11-03](#)

Secunia - Advisories - BNC IRC proxy "getnickuserhost()" Buffer Overflow Vulnerability

[web.archive.org](#)  
[text/html](#)

[SECUNIA 13149](#)

Debian -- Security Information -- DSA-595-1 bnc

[www.debian.org](#)  
[Deprecated Link](#)

[DEBIAN DSA-595](#)

[text/html](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com) [XF bnc-irc-getnickuserhost-bo\(18013\)](#)[text/html](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.2.4   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.4.6   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.4.8   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6     | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6.2   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6.4   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.8.8   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.8.9   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.2.4   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.4.6   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.4.8   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6     | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6.2   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.6.4   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.8.8   | All    | All     | All      |
| Application      | <a href="#">Bnc</a>    | <a href="#">Bnc</a>          | 2.8.9   | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | alpha   | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | arm     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | hppa    | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | ia-32   | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | ia-64   | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 3.0     | All    | m68k    | All      |

|                                |        |              |     |     |        |     |
|--------------------------------|--------|--------------|-----|-----|--------|-----|
| Operating System               | Debian | Debian Linux | 3.0 | All | mips   | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | mipsel | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | ppc    | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | s-390  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | sparc  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | alpha  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | arm    | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | hppa   | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | ia-32  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | ia-64  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | m68k   | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | mips   | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | mipsel | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | ppc    | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | s-390  | All |
| Operating System               | Debian | Debian Linux | 3.0 | All | sparc  | All |
| Operating System               | Gentoo | Linux        | All | All | All    | All |
| Operating System               | Gentoo | Linux        | All | All | All    | All |
| cpe:2.3:a:bnc:bnc:2.2.4:*****: |        |              |     |     |        |     |
| cpe:2.3:a:bnc:bnc:2.4.6:*****: |        |              |     |     |        |     |
| cpe:2.3:a:bnc:bnc:2.4.8:*****: |        |              |     |     |        |     |
| cpe:2.3:a:bnc:bnc:2.6:*****:   |        |              |     |     |        |     |
| cpe:2.3:a:bnc:bnc:2.6.2:*****: |        |              |     |     |        |     |
| cpe:2.3:a:bnc:bnc:2.6.4:*****: |        |              |     |     |        |     |

|                                                     |
|-----------------------------------------------------|
| cpe:2.3:a:bnc:bnc:2.8.*:*:*:*:*:                    |
| cpe:2.3:a:bnc:bnc:2.8.9.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.2.4.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.4.6.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.4.8.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.6.*:*:*:*:*:                    |
| cpe:2.3:a:bnc:bnc:2.6.2.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.6.4.*:*:*:*:*:                  |
| cpe:2.3:a:bnc:bnc:2.8.*:*:*:*:*:                    |
| cpe:2.3:a:bnc:bnc:2.8.9.*:*:*:*:*:                  |
| cpe:2.3:o:debian:debian_linux:3.0:*:alpha.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:arm.*:*:*:*:    |
| cpe:2.3:o:debian:debian_linux:3.0:*:hppa.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:ia-32.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:ia-64.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:m68k.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:mips.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:mipsel.*:*:*:*: |
| cpe:2.3:o:debian:debian_linux:3.0:*:ppc.*:*:*:*:    |
| cpe:2.3:o:debian:debian_linux:3.0:*:s-390.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:sparc.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:alpha.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:arm.*:*:*:*:    |
| cpe:2.3:o:debian:debian_linux:3.0:*:hppa.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:ia-32.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:ia-64.*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:m68k.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:mips.*:*:*:*:   |
| cpe:2.3:o:debian:debian_linux:3.0:*:mipsel.*:*:*:*: |

|                                                       |
|-------------------------------------------------------|
| cpe:2.3:o:debian:debian_linux:3.0:*:*:mipsel:*:*:*:*: |
| cpe:2.3:o:debian:debian_linux:3.0:*:*:ppc:*:*:*:*:    |
| cpe:2.3:o:debian:debian_linux:3.0:*:*:s-390:*:*:*:*:  |
| cpe:2.3:o:debian:debian_linux:3.0:*:*:sparc:*:*:*:*:  |
| cpe:2.3:o:gentoo:linux:*:*:*:*:*:                     |
| cpe:2.3:o:gentoo:linux:*:*:*:*:*:                     |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)