

# [NEWS] User Posting Vulnerability in Nick.com Forums (Nickelodeon)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0060.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/14/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Mon, 14 Jan 2002 14:35:02 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

User Posting Vulnerability in Nick.com Forums (Nickelodeon)

---

## SUMMARY

<<http://Nick.com>> Nick.com is a website for Kids whom watch the Nickelodeon cable channel. They offer a message board area that is moderated heavily to try to make it one of the safest areas on the net. A security vulnerability in the handling of incoming messages allows impersonation – writing messages with someone else nickname.

## DETAILS

When you create a user and log in to their message board system (powered by PeopleLink), a JavaScript window pops up with the forum selection and main content inside. This does not work too well with window resizing/scrolling in Mac OS X (or any other OS) so we chose to open the JavaScript's HTML contents in a new window. This helped the problem, but revealed a major flaw in their user identification system. The URL is formed like this:

<http://plnk.peoplelink.com/plnk/nickelodeon/boards40/frame.cfm?>

handle=ANY\_USERNAME\_HERE

&intgroup=100000910

Securiteam: [NEWS] User Posting Vulnerability in Nick.com Forums (Nickelodeon)

Handle means the Username of the poster. "intgroup" is the Forum/Message ID. You can change the "handle" part of the URL to ANY name, including already registered names – you then can post as any username. All messages take up to 24 hours to be "approved," but if the message is "clean," it usually will be approved, even if the name is a fake one. This has been tested. It was obvious that this was hidden in a JavaScript popup to probably cover this flaw.

Vendor status:

The webmaster has been contacted. A fix should be already in place.

Fix:

Nick.com forum moderators have confirmed they will be switching to a new message board system, and leaving all former data behind.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[danny@dricci.com](mailto:danny@dricci.com)> Danny Ricci.

=====

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)

=====  
=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Vulnerability Found in Frox Transparent FTP Proxy"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)