

# [UNIX] Nstxd Security Vulnerability (DoS)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0096.html>

---

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

**Date:** 03/31/04

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

Date: 31 Mar 2004 11:36:35 +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>

-----

Nstxd Security Vulnerability (DoS)

---

## SUMMARY

<<http://debmail.dereference.de/nstx/>> Nstxd is "the server from the Nstx project. Nstx can be used to create IP traffic over DNS (can be used by blackhats for special Wifi networks with DNS open for everybody)".

Unexpected input may crash the server called nstxd that will at least result in a DoS due to a NULL-pointer-reference. The service nstxd runs as root to bind the UDP port 53.

## DETAILS

Vulnerable Systems:

\* Nstx version 1.1-beta3

Immune Systems:

\* Nstx version 1.1-beta4

Vendor status:

The Nstx team quickly solved this bug. A new release is available: nstx-1.1-beta4.

From the ChangeLog:

Securiteam: [UNIX] Nstxd Security Vulnerability (DoS)

1.1-beta4: sky

2004/03/26

\* Fixed a remote DoS-Bug (NULL-pointer-dereference)

Solutions:

\* Upgrade your Nstx version at:

<<http://debmail.dereference.de/nstx/nstx-1.1-beta4.tgz>>

<http://debmail.dereference.de/nstx/nstx-1.1-beta4.tgz>

\* Workaround: Containment (chroot, jail...) and low level security solutions (grsecurity, systrace...) should be use to improve the security of such a server.

Example:

\*\* On the server (assume the IP is 192.168.1.34 for this example):

nstx-1.1-beta3# ./nstxd tun.mydomain.com

\*\* On a remote "evil" client:

remote-hacker\$ perl -e '{ print "A" x 500 }' | nc -u 192.168.1.34 53

This segfaults the server. This vulnerability might be dangerous as nstxd needs root privileges (to bind port 53). No exploit to get a remote shell has been reported (just a DoS).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:oudot@rstack.org>> Laurent Oudot.

=====

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.