

# [UNIX] InetUtils TFTP Client DNS Resolving Buffer Overflows

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0061.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 11/17/04

To: list@securiteam.com

Date: 17 Nov 2004 16:34:09 +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>

-----

InetUtils TFTP Client DNS Resolving Buffer Overflows

---

## SUMMARY

<<http://www.gnu.org/software/inetutils/inetutils.html>> InetUtils is "a collection of common network programs, among other TFTP". Untrusted data from DNS resolved hostname is copied into finite static buffers without any bounds checking. We can overflow several buffers located in the .bss. Also located in the .bss are function pointers used to implement FTP commands, so exploitation with code execution is possible.

## DETAILS

Vulnerable Systems:

- \* InetUtils version 1.4.2 and prior

The overflows all occur thanks to gethostbyname() returned data. Instead of copying that data using the length of the destination buffer, the length of the source buffer is used instead, or no length at all in the case of strcpy(). An attacker could configure their DNS server maliciously, or a local attacker on a LAN could spoof replies to neighbors to exploit this.

## Securiteam: [UNIX] InetUtils TFTP Client DNS Resolving Buffer Overflows

```
main.c:227: bcopy(host->h_addr, &peeraddr.sin_addr, host->h_length);
main.c:228: strcpy(hostname, host->h_name);
main.c:366: bcopy(hp->h_addr, (caddr_t)&peeraddr.sin_addr, hp->h_length);
main.c:369: strcpy(hostname, hp->h_name);
main.c-457: bcopy(hp->h_addr, (caddr_t)&peeraddr.sin_addr, hp->h_length);
main.c:461: strcpy(hostname, hp->h_name);
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:infamous41md@hotpop.com>>  
sean.

=====

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.