

# [UNIX] Linux Package Default UID (573)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0117.html>

---

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

*Date:* 12/27/01

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

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

Date: Thu, 27 Dec 2001 07:27:02 +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.

-----

Linux Package Default UID (573)

---

## SUMMARY

Whenever the source code of Linux is decompressed, it will turn out with both UID of 573 and GID of 573. This by itself is not a security vulnerability, however, if a user with UID of 573 exists (or that belongs to GID 573) he will be able to modify the source code, allowing him to insert hostile code into it (if the default UID/GID are not changed).

## DETAILS

Example:

```
/usr/src# tar xzf linux-2.4.16.tar.gz
```

```
/usr/src# cd linux
```

```
/usr/src/linux# ls -l
```

```
total 3204
```

```
-rw-r--r-- 1 573 573 18689 Oct 9 18:00 COPYING
```

```
-rw-r--r-- 1 573 573 77693 Nov 11 13:09 CREDITS
```

```
drwxr-xr-x 28 573 573 4096 Nov 22 13:53 Documentation/
```

```
-rw-r--r-- 1 573 573 38940 Nov 16 13:03 MAINTAINERS
```

```
-rw-r--r-- 1 573 573 14242 Oct 5 15:10 README
```

```
-rw-r--r-- 1 573 573 2815 Apr 6 2001 REPORTING-BUGS
```

```
-rw-r--r-- 1 573 573 8884 Mar 6 2001 Rules.make
```

```
drwxr-xr-x 17 573 573 4096 Feb 13 2001 arch/
```

```
drwxr-xr-x 39 573 573 4096 Dec 21 21:05 drivers/
```

## Securiteam: [UNIX] Linux Package Default UID (573)

```
drwxr-xr-x 45 573 573 4096 Dec 21 21:29 fs/  
drwxr-xr-x 25 573 573 4096 Dec 21 21:13 include/  
drwxr-xr-x 2 573 573 4096 Dec 21 21:14 init/  
drwxr-xr-x 2 573 573 4096 Dec 21 21:37 ipc/  
drwxr-xr-x 2 573 573 4096 Dec 21 21:15 kernel/  
drwxr-xr-x 2 573 573 4096 Dec 21 21:37 lib/  
drwxr-xr-x 2 573 573 4096 Dec 21 21:22 mm/  
drwxr-xr-x 28 573 573 4096 Dec 21 21:37 net/  
drwxr-xr-x 5 573 573 4096 Dec 21 21:13 scripts/  
/usr/src/linux#
```

As you can see, the UID and GID are both set to 573, if the administrator does not change this to his own UID or, any other known-safe UID, an attacker with that UID can modify the source code of Linux and insert his own code into it.

### Workaround:

It is encouraged that all administrators execute the following command after unpacking the Linux source code (or any other source code downloaded off the Internet):

```
# chown root.root /usr/src/linux -R
```

### ADDITIONAL INFORMATION

The information has been provided by Gobbles.

=====

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] PFinger Format String Vulnerability"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)