

# [UNIX] Apache Local User to Root Escalation

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00053.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 26 Mar 2007 22:18:21 +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>

-----

Apache Local User to Root Escalation

---

## SUMMARY

A vulnerability in way debian's version of Apache handles cttys allows local users to gain elevated privileges if the root has manually restarted the Apache service.

## DETAILS

Vulnerable Systems:

- \* Apache version 1.3.34–4 (Debian only)

Unlike every other daemon, apache does not abdicate its controlling tty on startup, and allows it to be inherited by a cgi script (for example, a local user's CGI executed using suexec). When apache is manually restarted, the inherited ctty is the stdin of the (presumably root) shell that invoked the new instance of apache. Any process is permitted to invoke the TIOCSTI ioctl on the fd corresponding to its ctty, which allows it to inject characters that appear to come from the terminal master. Thus, a user created CGI script can inject and have executed any input into the shell that spawned apache.

[UNIX] Apache Local User to Root Escalation

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ret28@xxxxxxxxxx>> Richard Thripleton.

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

**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.