

Why can setuid programs regain root after dropping it when using capabilities?

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-11/9611.html>

From: David Chau (ddcc_at_mit.edu)

Date: 11/30/05

Date: Tue, 29 Nov 2005 21:35:45 -0500

To: linux-kernel@vger.kernel.org

Hi,

While debugging some code, I found that a setuid program could regain root after dropping root if the program used capabilities. (I tested this on 2.6.14 and 2.6.9.) Is this the expected behavior? Here's a short test case:

```
/* chown root this program, suid it, and run it as non-root */
#include <sys/types.h>
#include <sys/capability.h>
#include <unistd.h>
#include <stdio.h>
int main() {
    cap_set_proc(cap_from_text("all-eip")); /* drop all caps */
    setuid(getuid()); /* drop root. this call succeeds */
    setuid(0); /* this should fail! but doesn't */
    printf("%d\n", getuid()); /* we regained root. prints 0 */
    return 0;
}
```

(If we don't use capabilities at all, and take out the `cap_set_proc` line, then the program behaves as expected, and doesn't allow us to regain root.)

—David

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>