

[TOOL] Touch2, Change Last-inode-change Times on Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0086.html>

From: support@securiteam.com

Date: 06/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 19 Jun 2002 09:18:10 +0200 (CEST)

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.

Touch2, Change Last-inode-change Times on Files

DETAILS

Touch2 is a utility that modifies the ctime. Touch(1) can be used to change the last-access & last-modification times on the files (or directories) you read or modify, but doing this will change the last-inode-change time to the current time. Touch2 should be executed after touch(1) or other commands.

Tool code:

/*

* touch2

* Change last-inode-change times on files

*

* (!c) 2002 by Ighighi

* Venezuela

*

* Overview:

* You use touch(1) to change the last-access & last-modification times

* on the files (or directories) you read or modify. The problem is that

* doing this will change the last-inode-change time to the current time.

* Now you may use touch2 right after using touch(1) to erase all evidence.

Securiteam: [TOOL] Touch2, Change Last–inode–change Times on Files

```
* Stealth hacking is the motto!  
* It must be run as root!  
*/
```

```
#include <stdio.h>  
#include <stdlib.h>  
#include <string.h>  
#include <unistd.h>  
#include <sys/stat.h>  
#include <sys/time.h>  
#include <time.h>
```

```
static int change_ctime(const char *file, const struct timeval *ctime)  
{  
    struct timeval tv[2], now;  
    struct stat inode;  
  
    /* Get file's atime & mtime */  
    if (stat(file, &inode) < 0) return -1;  
  
    memset(&tv, 0, sizeof(tv));  
    /* st_[am]time may be either struct timespec or time_t  
    * the first member of struct timespec is tv_sec  
    * (the same as struct timeval)  
    */  
    memcpy(&tv[0], &inode.st_atime, sizeof(inode.st_atime));  
    tv[0].tv_usec /= 1000; /* nanosecs to microsecs */  
    memcpy(&tv[1], &inode.st_mtime, sizeof(inode.st_mtime));  
    tv[1].tv_usec /= 1000; /* nanosecs to microsecs */  
  
    /* Save current time */  
    if (gettimeofday(&now, NULL) < 0) return -1;  
  
    if (settimeofday(ctime, NULL) < 0) return -1;  
  
    if (utimes(file, tv) < 0) return -1;  
  
    /* Restore system time */  
    if (settimeofday(&now, NULL) < 0) return -1;  
  
    return 0;  
}
```

```
/* converts from "YYYY:MM:DD:hh:mm:ss:uuuuuu" to struct timeval */  
static void str2timeval(const char *s, struct timeval *tvp)  
{  
    struct tm tm;  
#define DELIM ':'  
  
    if (! tvp) return;
```

Securiteam: [TOOL] Touch2, Change Last-inode-change Times on Files

```
memset(&tm, 0, sizeof(tm));
if (s) {
    tm.tm_year = atoi(s) - 1900;
    if ( (s = strchr(s, DELIM)) ) {
        tm.tm_mon = atoi(++s) - 1;
        if ( (s = strchr(s, DELIM)) ) {
            tm.tm_mday = atoi(++s);
            if ( (s = strchr(s, DELIM)) ) {
                tm.tm_hour = atoi(++s);
                if ( (s = strchr(s, DELIM)) ) {
                    tm.tm_min = atoi(++s);
                    if ( (s = strchr(s, DELIM)) ) {
                        tm.tm_sec = atoi(++s);
                        if ( (s = strchr(s, DELIM)) ) {
                            tvp->tv_usec = atoi(++s);
                        }
                    }
                }
            }
        }
    }
}
tvp->tv_sec = mktime(&tm);

return;
}

static void exit_usage(int status)
{
    FILE *fp;

    if (status) fp = stderr;
    else fp = stdout;

    fprintf(fp, "touch2 by Ighighi \n");
    fprintf(fp, "Usage: ./touch2 [options] files... \n");
    fprintf(fp, " options: \n");
    fprintf(fp, " [-h] \n");
    fprintf(fp, " Print this help and exit \n");
    fprintf(fp, " [-r file] \n");
    fprintf(fp, " Use the ctime of the file instead of the current time
\n");
    fprintf(fp, " [-d YYYY[:MM[:DD[:hh[:mm[:ss[:uuuuu]]]]]]] \n");
    fprintf(fp, " Use the argument instead of the current time \n");

    exit(status);
}

int main(int argc, char *argv[])
{
    struct timeval new_ctime; /* New inode-change time */
```

Securiteam: [TOOL] Touch2, Change Last–inode–change Times on Files

```
char *rfile = NULL; /* Reference file */
struct stat inode;
int i;

for (i = 1; i < argc; i++) {
if (argv[i][0] == '-') {
    switch (argv[i][1]) {
        case 't': /* time */
            str2timeval(argv[++i], &new_ctime);
            break;
        case 'r': /* ref file */
            rfile = argv[++i];
            break;
        case 'h': /* help */
            exit_usage(0);
            break;
        default:
            exit_usage(1);
    }
}
else {
    break;
}
}

if (i >= argc) {
    exit_usage(1);
}

gettimeofday(&new_ctime, NULL);

if (rfile) {
    /* Get file's ctime */
    if (stat(rfile, &inode) < 0) {
        perror(rfile);
        exit(1);
    }

    memset(&new_ctime, 0, sizeof(new_ctime));
    /* st_ctime may be either struct timespec or time_t
    * the first member of struct timespec is tv_sec
    * (the same as struct timeval)
    */
    memcpy(&new_ctime, &inode.st_ctime, sizeof(inode.st_ctime));
    new_ctime.tv_usec /= 1000; /* nanosecs to microsecs */
}

for (; i < argc; i++) {
    if (change_ctime(argv[i], &new_ctime) < 0) {
        perror(argv[i]);
    }
}
```

Securiteam: [TOOL] Touch2, Change Last-inode-change Times on Files

```
}  
  
exit(0);  
}
```

ADDITIONAL INFORMATION

The information has been provided by Ighighi.

=====

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.

-
- *Previous message:* support@securiteam.com: "[NT] DeepMetrix LiveStats JavaScript Injection"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)