

[NT] Buffer Overflow Vulnerability in Microsoft Windows (CONSOLE_STATE_INFO, MS05-018)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/13/05

To: list@securiteam.com

Date: 13 Apr 2005 13:43:53 +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>

Buffer Overflow Vulnerability in Microsoft Windows (CONSOLE_STATE_INFO, MS05-018)

SUMMARY

The lack of range checking in Microsoft Windows API CONSOLE_STATE_INFO structure allows attackers or bad code to create a buffer overflow in one of the fields of the structure and may lead to a denial of service and also allow to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Windows 2000 SP4 CSRSS.EXE version 5.0.2195.6601
- * Windows 2000 SP4 WINSRV.DLL version 5.0.2195.6699
- * Windows XP SP1a CSRSS.EXE version 5.0.2195.6601
- * Windows XP SP1a WINSRV.DLL version 5.0.2195.6699

The Win32 application-programming interface (API) offers a console Windows feature that provides a means to implement command-line and other character-based user interfaces. The specific code for this feature within the Windows 2000, XP and 2003 operating systems resides in a core system process called CSRSS.EXE. This process is the main executable for the

Microsoft Client/Server Runtime Server Subsystem. The process manages most graphical commands in Windows.

Local exploitation of a stack-based buffer overflow vulnerability within various versions of Microsoft Windows operating system allows attackers to execute arbitrary code with SYSTEM privileges.

Console windows are created and managed by code in the WINSRV.DLL file that resides in the CSRSS.EXE process. This file contains the server-side version of the 32-bit user and GDI routines (graphics engine). When a user selects the "Properties" item from the system menu of a console window, a data structure containing information about the console window is copied into the file-mapping object. The text of an assert in the checked build appears to indicate that this structure is called CONSOLE_STATE_INFO, which has the following structure:

```
typedef struct _CONSOLE_STATE_INFO
{
/* 0x00 */ DWORD cbSize;
/* 0x04 */ COORD ScreenBufferSize;
/* 0x08 */ COORD WindowSize;
/* 0x0c */ POINT WindowPosition;
/* 0x14 */ COORD FontSize;
/* 0x18 */ DWORD FontFamily;
/* 0x1c */ DWORD FontWeight;
/* 0x20 */ WCHAR FaceName[32]; /* Buffer Overflow */
/* 0x60 */ DWORD CursorSize;
/* 0x64 */ BOOL FullScreen;
/* 0x68 */ BOOL QuickEdit;
/* 0x6c */ BOOL DefaultWindowPos;
/* 0x70 */ BOOL InsertMode;
/* 0x74 */ WORD ScreenColors;
/* 0x76 */ WORD PopupColors;
/* 0x78 */ BOOL HistoryNoDup;
/* 0x7c */ DWORD HistoryBufferSize;
/* 0x80 */ DWORD NumberOfHistoryBuffers;
/* 0x84 */ COLORREF ColorTable[16];
/* 0xc4 */ DWORD CodePage;
/* 0xc8 */ DWORD hwnd;
/* 0xcc */ WCHAR ConsoleTitle[2];
} CONSOLE_STATE_INFO, *PCONSOLE_STATE_INFO;
```

The values contained within this struct are passed as a file-mapping object to code within WINSRV.DLL that does not properly validate the data. Passing a CONSOLE_STATE_INFO of all zero's can induce an integer divide-by-zero exception in the CSRSS process that will cause the process to terminate and the system to crash (blue screen) shortly thereafter. The CONSOLE_STATE_INFO data structure contains a null terminated string specifying the name of a font, FaceName[32]. This string is copied into a fixed sized stack buffer without any sanity checking via the wcsncpy() function, as can be seen in the following assembly excerpt from WINSRV.DLL

Securiteam: [NT] Buffer Overflow Vulnerability in Microsoft Windows (CONSOLE_STATE_INFO, MS05-018)

on Windows 2000 Service Pack 4 Checked Build:

```
0x5FFB39DF push [ebp+lpFaceName]
0x5FFB39E2 lea eax, [ebp-54h]
0x5FFB39E5 push eax
0x5FFB39E6 call j_wcsncpy
```

By supplying a string longer than 32 bytes, an attacker can trigger the stack-based buffer overflow to gain control of the computer and eventually execute arbitrary code.

Exploitation allows local unprivileged users to potentially execute arbitrary code on affected systems with SYSTEM privileges. An attacker with non-privileged access to a vulnerable system can leverage this vulnerability to fully compromise the underlying system. Exploitation of the described vulnerability requires that the attacker be able to create a console window. This attack may be used on public terminals to break imposed restrictions that otherwise prevent users from fully controlling the computer.

Workaround:

Restrict console access on public terminals where security is a concern. This can be accomplished by creating the following registry key:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System

Add a DWORD named DisableCMD with the value "1" to disable command prompt and batch files or the value "2" to disable command prompt but allow batch files.

Vendor Status:

The vendor has released updated for the following systems:

* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=992C1BF9-A2C0-49D2-9059-A1DAD6703213>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=992C1BF9-A2C0-49D2-9059-A1DAD6703213>

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F0683E2B-8E8F-474F-B8D8-46C4C33FCE99>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=F0683E2B-8E8F-474F-B8D8-46C4C33FCE99>

* Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B52F9281-570F-4F7A-8DEF-5AEAB6E8E002>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=B52F9281-570F-4F7A-8DEF-5AEAB6E8E002>

* Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C51D6AD5-93BA-4717-A5DB-5CE78F70592E>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=C51D6AD5-93BA-4717-A5DB-5CE78F70592E>

Securiteam: [NT] Buffer Overflow Vulnerability in Microsoft Windows (CONSOLE_STATE_INFO, MS05-018)

* Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E66332D4-3952-428F-AC62-AC8124F8942A>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=E66332D4-3952-428F-AC62-AC8124F8942A>

* Microsoft Windows Server 2003 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C51D6AD5-93BA-4717-A5DB-5CE78F70592E>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=C51D6AD5-93BA-4717-A5DB-5CE78F70592E>

Disclosure Timeline:

- 01/04/2005 – Initial vendor notification
- 01/04/2005 – Initial vendor response
- 04/12/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:labs-no-reply@idefense.com>>
iDEFENSE Labs.

The information has been provided by iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=230&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=230&type=vulnerabilities>

=====

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.