

[NT] Microsoft Windows Task Scheduler '.job' Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0059.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/14/04

To: list@securiteam.com

Date: 14 Jul 2004 18:31:29 +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 Task Scheduler '.job' Stack Overflow

SUMMARY

The Microsoft Windows operating system provides a service which is designed to run a particular application at a given time or date – the Task Scheduler. When a new task is added through the control panel application, a '.job' file containing this information is created and stored in the 'Tasks' folder in the Windows directory.

It has been found that it is possible to create a specially crafted '.job' file which could allow local or remote code execution using a number of different applications as the attack vectors.

DETAILS

By crafting a '.job' file which contains overly long parameters, stack based buffers can be overflowed, resulting in critical information, including a saved return address or a structured exception handler structure being completely overwritten, allowing an attacker to direct the code execution flow to an address of their choosing. If the file contains arbitrary executable code, the process can be forced to execute this allowing, in worst cases, complete control over the target system.

Securiteam: [NT] Microsoft Windows Task Scheduler '.job' Stack Overflow

The actual vulnerability arises from a lack of boundary checking performed when copying the information out of memory containing the contents of the file into the stack-based buffers.

In some circumstances the overflow is triggered automatically when viewing the directory that contains the job file in an explorer window due to the fact that 'shell32.dll' will detect the '.job' file extension, and load 'mstask.dll' allowing the module to examine the file, which is when the overflow occurs.

Due to the fact that the overflow is triggered by a module loaded within the process space of another running executable, any code which would be executed by exploiting this flaw will be run with the privileges of the user running that application, in the most common cases this would be the user logged on to the machine.

Two applications that have been successfully tested as vectors for exploiting this issue are Windows Explorer and Internet Explorer – when attempting to view network shares containing the '.job' file. File sharing through MSN Messenger has also been proven to be an effective vector for attack. In the case of Internet Explorer, this issue could be exploited simply by viewing a website containing a frame pointing to a network share containing the '.job' file. Please note that there are many other ways of exploiting this issue, this is certainly not an exhaustive list.

Fix Information:

Microsoft have provided a fix for this issue which can be downloaded from the Microsoft Security website at:

<<http://www.microsoft.com/technet/security/bulletin/ms04-022.msp>>
<http://www.microsoft.com/technet/security/bulletin/ms04-022.msp>

ADDITIONAL INFORMATION

The information has been provided by <mailto:peter@ngssoftware.com> Peter Winter-Smith.

The original article can be found at:

<<http://www.ngssoftware.com/advisories/mstaskjob.txt>>
<http://www.ngssoftware.com/advisories/mstaskjob.txt>

=====

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.

Securiteam: [NT] Microsoft Windows Task Scheduler '.job' Stack Overflow

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.