

[NT] Microsoft IIS ssinc.dll Over-long Filename Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0066.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/30/03

To: list@securiteam.com

Date: 30 May 2003 23:07:35 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Microsoft IIS ssinc.dll Over-long Filename Buffer Overflow Vulnerability

SUMMARY

NSFOCUS Security Team has found a buffer overflow vulnerability in the way a dynamic linking library (ssinc.dll) that is shipped with Microsoft IIS 4.0/5.0 handles the files it parsers. Exploiting the vulnerability would allow local attackers to gain SYSTEM privileges.

DETAILS

Microsoft IIS supports SSI (Server Side Include) functionality. The ssinc DLL is a SSI interpreter. By default the extended names .stm,.shtm and shtml will be mapped to interpreter (ssinc.dll).

SSI supports the "#include" command. Typically, it is used in the following manner:

```
<!--#include file="filename"-->
```

The interpreter's handling of the "#include" command first requires it to

Securiteam: [NT] Microsoft IIS ssinc.dll Over-long Filename Buffer Overflow Vulnerability

attempt to gain the physical path of the shtml file, to do so it will copy the URI request to a buffer of a fixed size.

For example, when requesting the following shtml file:

<http://iishost/abc/test.shtml>, it will copy the string "/abc/test.shtml" to the buffer.

Because the length of the shtml filename is not been checked during the copy procedure, it can cause a stack overflow.

NSFocus Security Team has found a similar problem in the past. See:

<http://www.nsfocus.net/index.php?act=advisory&do=view&adv_id=17>

http://www.nsfocus.net/index.php?act=advisory&do=view&adv_id=17, and the corresponding Microsoft Security Bulletin is found at:

<<http://www.microsoft.com/technet/security/bulletin/ms01-044.asp>>

<http://www.microsoft.com/technet/security/bulletin/ms01-044.asp>

Microsoft's pervious patch to IIS has involved checking for an over-long shtml filename in order to avoid a buffer overflow. Whenever an overly long shtml filename is found, it will shorten the filename to a legal length, and then attempt to open it. However, after it has been successful in opening the file, the ssinc.dll will revert back to the original filename (which can be overly long).

Therefore, by creating a WEB file with a special length, local attackers could bypass the check, then request a shtml file with an overly long filename to cause a buffer overflow, this in turn causes IIS cease to respond. By carefully constructing the overflow data, attackers could run arbitrary code with local SYSTEM privileges.

However, two conditions are required to carry out the attack:

1. Attackers need to have the privilege to create files on web directory.
2. Attackers need to be able to access the created files via the web site.

Workaround:

1. Disable untrusted users' writing privileges to web directory.
2. If SSI functionality is not required, remove .shtml, .shtm, .stm mapping.

3. Install IIS Lockdown tools provided by Microsoft:

<<http://www.microsoft.com/downloads/details.aspx?familyid=dde9efc0-bb30-47eb-9a61-fd755d23cdec&displaylang=en>>

<http://www.microsoft.com/downloads/details.aspx?familyid=dde9efc0-bb30-47eb-9a61-fd755d23cdec&displaylang=en>

Vendor Status:

2002.11.05 Informed vendor about the issue

2003.05.28 Microsoft has issued a Security Bulletin (MS03-018) and the related patch.

Detailed Microsoft Security Bulletin is available at:

<<http://www.microsoft.com/technet/security/bulletin/ms03-018.asp>>

<http://www.microsoft.com/technet/security/bulletin/ms03-018.asp>

Securiteam: [NT] Microsoft IIS ssinc.dll Over-long Filename Buffer Overflow Vulnerability

Patches are available at:

<<http://microsoft.com/downloads/details.aspx?FamilyId=2F5D9852-4ADD-44F8-8715-AC3D7D7D94BE>>
<http://microsoft.com/downloads/details.aspx?FamilyId=2F5D9852-4ADD-44F8-8715-AC3D7D7D94BE>

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@nsfocus.com>
NSFOCUS Security Team.

=====

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.