

[NT] Windows 2000 and NT4 IIS .HTR Remote Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0046.html>

From: support@securiteam.com

Date: 06/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 13 Jun 2002 00:35:26 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Windows 2000 and NT4 IIS .HTR Remote Buffer Overflow

SUMMARY

A vulnerability in transfer chunking, in combination with the processing of HTR request sessions can be exploited to remotely execute code of an attackers choice on the vulnerable machine. By sending a carefully crafted session, an attacker can overwrite a section of the heap. Data structures in the overwritten heap can be manipulated to move attacker-supplied data to attacker supplied memory addresses, thereby altering the flow of execution into an attacker supplied payload.

DETAILS

Systems Affected:

Microsoft Windows NT 4.0 Internet Information Services 4.0

Microsoft Windows 2000 Internet Information Services 5.0

The following example will show the vulnerable condition. The dllhost.exe child process will silently die because the developers have replaced the default exception filter. So if you want to examine this closer, load a debugger up on the dllhost child process before you send this example session over the wire.

Securiteam: [NT] Windows 2000 and NT4 IIS .HTR Remote Buffer Overflow

```
*****Begin Session*****
POST /EEYE.htr HTTP/1.1
Host: 0day.big5.com
Transfer-Encoding: chunked

20
XXXXXXXXXXXXXXXXXXXXXXXXXXXXEYE2002
0
[enter]
[enter]
*****End Session*****
```

Technical Description:

The example session above overwrites a section of the heap that contains data structures related to the memory management system. By manipulating the content of these structures we can overwrite an arbitrary 4 bytes of memory with an attacker supplied address.

While many may believe that the risk for these types of vulnerabilities is fairly low due to the fact that addressing is dynamic and brute force techniques would need to be use in an attack, eEye strongly disagrees. This premise is false as successful exploitation can be made with one attempt, across dll versions. An attacker can overwrite static global variables, stored function pointers, process management structures, memory management structures, or any number of data types that will allow him to gain control of the target application in one session.

Vendor Status:

Microsoft has released a security bulletin and patch:

<<http://www.microsoft.com/technet/security/>>
<http://www.microsoft.com/technet/security/>

Beyond installing the Microsoft security patch it is also recommend to disable the .htr ISAPI filter if you have not already done so. Microsoft's security advisory references more information on the steps of how to disable the .htr ISAPI filter.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ryan@eeye.com>> Ryan Permech of eEye.

=====

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: [NT] Windows 2000 and NT4 IIS .HTR Remote Buffer Overflow

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.

- ***Previous message:*** support@securiteam.com: "[NT] Unchecked Buffer in SQLXML Could Lead to Code Execution"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)