

Securiteam: [NT] Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

[NT] Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/17/05

To: list@securiteam.com

Date: 17 Apr 2005 17:08:51 +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>

Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

SUMMARY

The heap corruption and race condition in Internet Explorer allow attackers to execute arbitrary code in the Windows operating system.

DETAILS

Vulnerable Systems:

- * Windows XP with Internet Explorer 6.0.2180
- * Windows XP Professional with Service Pack 2
- * Windows XP Professional with Service Pack 1
- * Windows 2000 Professional with Service Pack 4

Heap Corruption:

The vulnerability specifically exists in the handling of long host-names.

When IE is requested to open a URL with a host-name part longer than about 256 characters, the heap becomes slightly corrupted. This corruption may cause no visible effect, or it may cause the Address Bar to contain a URL with "garbage" characters as the host-name. It may also cause IE to crash, referencing an invalid memory address. In testing done, the addresses

Securiteam: [NT] Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

referred during a crash are at times controllable by the web page containing the malformed URL.

Remote exploitation of an input validation error in Microsoft Internet Explorer allow the execution of arbitrary code.

Although it is not trivial to exploit this vulnerability, it is believed to be possible. Testing during verification of this vulnerability revealed multiple situations where remotely supplied values were used to reference memory locations. A remote attacker may be able to read data from, write data to, or execute arbitrary code by supplying specifically malformed content.

Successful exploitation allows remote attackers to execute arbitrary code under the privileges of the current user.

Workaround:

Although it will not prevent all means of exploitation, disable active scripting if it is not necessary for day-to-day operations using the following steps:

1. In IE, click on Tools and select Internet Options from the drop-down menu.
2. Click the Security tab and the Custom Level button.
3. Under Scripting, then Active Scripting, click the Disable radio button.

Race Condition:

Internet Explorer supports dynamic creation of HTML elements with JavaScript using various DHTML methods such as `createElement()`, `appendChild()`, and `removeNode()`. A number of problems have been found in the implementation of these objects and methods, including some which can be exploited to cause execution of arbitrary code.

The problem specifically exists within the memory management routines of Internet Explorer's object handling code. In some situations one thread reads data from memory that has either been overwritten by another thread or has not yet been initialized by another thread. This can lead to random crashes and remote command execution.

Remote exploitation of a race condition vulnerability in version 6 of Microsoft Internet Explorer web browser could allow the execution of arbitrary code under the privileges of the currently logged in user.

In order to exploit this vulnerability an attacker must convince the victim to visit a web site, or cause malicious DHTML code to be rendered by Internet Explorer using some other technique, such as a persist cross-site scripting attack on a trusted site.

Successful exploitation allows remote attackers to execute arbitrary code in the context of the user running the Internet Explorer process. Exploitation will not be 100% reliable. However, proof of concept exploit

Securiteam: [NT] Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

code was generated with reliable execution approximately 90% of the time.

Workaround:

Disable active scripting, if it is not necessary for daily operations, using the following steps:

1. In IE, click on Tools and select Internet Options from the drop-down menu.
2. Click the Security tab and the Custom Level button.
3. Under Scripting, then Active Scripting, click the Disable radio button.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0553>>

CAN-2005-0553

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0554>>

CAN-2005-0554

Vendor Status:

The vendor has released updates for the following systems:

- * Internet Explorer 5.01 Service Pack 3 on Microsoft Windows 2000 Service Pack 3:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6CF45449-03D8-40B8-A4C0-09F413EE8EAB>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6CF45449-03D8-40B8-A4C0-09F413EE8EAB>

- * Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=627F8991-7717-4ADE-A5AE-169591B6AAE0>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=627F8991-7717-4ADE-A5AE-169591B6AAE0>

- * Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 3, on Microsoft Windows 2000 Service Pack 4, or on Microsoft Windows XP Service Pack 1:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=92E5A83D-9131-4B20-915A-A444C51656DC>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=92E5A83D-9131-4B20-915A-A444C51656DC>

- * Internet Explorer 6 Service Pack 1 for Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium):

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=87241BC0-E1E9-4EFC-A6EC-5413119D3100>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=87241BC0-E1E9-4EFC-A6EC-5413119D3100>

- * Internet Explorer 6 for Microsoft Windows Server 2003:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=88879B7A-3F4D-40D4-ADFD-4BBD8D4D865F>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=88879B7A-3F4D-40D4-ADFD-4BBD8D4D865F>

- * Internet Explorer 6 for Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium):

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FF80E80F-862A-4484-BC9D-FE05F966F1F4>>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FF80E80F-862A-4484-BC9D-FE05F966F1F4>

- * Internet Explorer 6 for Microsoft Windows XP Service Pack 2:

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=974F9611-6352-4F9C-B258-346C317857C5>>

Securiteam: [NT] Multiple Vulnerabilities in Internet Explorer (Heap Corruption, Race Condition)

<http://www.microsoft.com/downloads/details.aspx?FamilyId=974F9611-6352-4F9C-B258-346C317857C5>

Disclosure Timeline:

10/25/2004 – Initial vendor notification and Initial vendor response for the Race Condition advisory

11/11/2004 – Initial vendor notification and Initial vendor response for the Heap Corruption advisory

04/12/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs-advisories@idefense.com> idlabs.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=228&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=228&type=vulnerabilities> and at
<<http://www.idefense.com/application/poi/display?id=229&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=229&type=vulnerabilities>

The SecuriTeam advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/5AP0B0UFFM.html>>
<http://www.securiteam.com/windowsntfocus/5AP0B0UFFM.html>

=====

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.