

memory addresses and redirect process execution to attacker-specified arbitrary code. This would result in arbitrary code execution if successful, allowing an attacker to gain unauthorized access to the affected computer.

This issue is reported to affect Microsoft Internet Explorer 6 running on a Windows 2000 SP4 platform.

Attack Scenarios

To carry out this attack, the attacker crafts a malicious HTML file containing a malformed IFRAME tag. This tag specifies large string values for the 'SRC' and 'NAME' properties.

An attacker hosts this file on a Web server and entices a user to visit the malicious site.

If successful, this attack results in crashing the user's browser. If the attacker is able to overwrite sensitive memory addresses, this issue may result in arbitrary code execution in the context of the user running the browser.

Exploits

A proof of concept is available from the following location:

http://felinemenace.org/~nd/crash_ie/2446.html

An exploit has been made available. Please see the referenced message for more information.

Mitigating Strategies

Run all client software as a non-privileged user with minimal access rights.

Running the client browser as a user with the minimal amount of privileges can reduce the impact of latent vulnerabilities.

Do not accept or execute files from untrusted or unknown sources.

Users should refrain from opening or executing files originating from untrusted or unknown sources.

Do not follow links provided by unknown or untrusted sources.

An attacker may supply a link to a malicious Web site that is designed to trigger this issue. Users should refrain from following links that originate from untrusted sources.

Solutions

Currently we are not aware of any vendor-supplied patches for this issue. If you feel we are in error or are aware of more recent information, please mail us at: vuldb@securityfocus.com <<mailto:vuldb@securityfocus.com>>.

Credit

This issue was reported by ned <nd@felinemenace.org> and Berend-Jan Wever <skylined@edup.tudelft.nl>.

Change Log

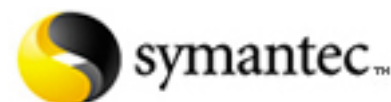
2004.11.02: An exploit has become available.

2004.10.25: Initial analysis.

URL

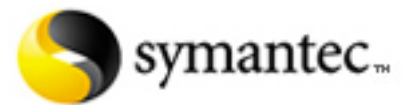
<https://alerts.symantec.com/members/viewfile.asp?guid=5532F9F079EF4955A508A35A67CC5452>

Microsoft Internet Explorer Malformed IFRAME Remote Buffer
Overflow Vulnerability



Create Date 11/2/2004 2:50:20 PM GMT

Microsoft Internet Explorer Malformed IFRAME Remote Buffer
Overflow Vulnerability



Create Date 11/2/2004 2:50:20 PM GMT