

[NT] Flaw in Windows Script Engine Could Allow Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0065.html>

From: support@securiteam.com

Date: 03/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Mar 2003 12:38:20 +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

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

Flaw in Windows Script Engine Could Allow Code Execution

SUMMARY

The Windows Script Engine provides Windows operating systems with the ability to execute script code. Script code can be used to add functionality to web pages, or to automate tasks within the operating system or within a program. Script code can be written in several different scripting languages, such as Visual Basic Script, or JScript.

A flaw exists in the way by which the Windows Script Engine for JScript processes information. An attacker could exploit the vulnerability by constructing a web page that, when visited by the user, would execute code of the attacker's choice with the user's privileges. The web page could be hosted on a web site, or sent directly to the user in email.

Although Microsoft has supplied a patch for this vulnerability and recommends all affected customers install the patch immediately, additional preventive measures have been provided so that customers can use to help block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch. These temporary

Securiteam: [NT] Flaw in Windows Script Engine Could Allow Code Execution

workarounds are discussed in the "Workarounds" section in the FAQ below.

DETAILS

Affected Software:

- * Microsoft Windows 98
- * Microsoft Windows 98 Second Edition
- * Microsoft Windows Me
- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0 Terminal Server Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP

Mitigating factors:

- * For an attack to be successful, the user would need to visit a website under the attacker's control or receive an HTML e-mail from the attacker.
- * Computers configured to disable active scripting in Internet Explorer are not susceptible to this issue.
- * Exploiting the vulnerability would allow the attacker only the same privileges as the user. Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges.
- * Automatic exploitation of the vulnerability by an HTML email would be blocked by Outlook Express 6.0 and Outlook 2002 in their default configurations, and by Outlook 98 and 2000 if used in conjunction with the Outlook Email Security Update.

Patch availability:

Download locations for this patch

The patches for all Windows systems are available via Windows Update. In addition, these patches are also available for download to allow the patches to be manually installed.

- * Windows 98 and Windows 98 SE:

<http://www.microsoft.com/windows98/downloads/contents/WUCritical/q814078/default.asp>
<http://www.microsoft.com/windows98/downloads/contents/WUCritical/q814078/default.asp>

- * Windows Me:
- * Windows Update.

- * Windows NT 4.0:

<http://microsoft.com/downloads/details.aspx?FamilyId=C6504FD9-5E2C-45BF-9424-55D7C5D2221B&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=C6504FD9-5E2C-45BF-9424-55D7C5D2221B&displaylang=en>

- * Windows NT 4.0, Terminal Server Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=C6504FD9-5E2C-45BF-9424-55D7C5D2221B&displaylang=en>
<http://microsoft.com/downloads/details.aspx?FamilyId=C6504FD9-5E2C-45BF-9424-55D7C5D2221B&displaylang=en>

Securiteam: [NT] Flaw in Windows Script Engine Could Allow Code Execution

* Windows 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=824B1BD4-B4D6-49D5-8C58-199BDC731B64&displayla>
<http://microsoft.com/downloads/details.aspx?FamilyId=824B1BD4-B4D6-49D5-8C58-199BDC731B64&displaylan>

* Windows XP Home Edition and Professional Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=824B1BD4-B4D6-49D5-8C58-199BDC731B64&displayla>
<http://microsoft.com/downloads/details.aspx?FamilyId=824B1BD4-B4D6-49D5-8C58-199BDC731B64&displaylan>

What's the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could cause code of his or her choice to be executed as though it originated on the local machine.

What causes the vulnerability?

The vulnerability is caused by a heap overflow in the Windows Script Engine for the JScript scripting language, JScript.dll.

What is a scripting language?

Scripting languages can be used to add additional functionality to HTML web pages or operating systems. They can enable a web author to set and store variables, and work with data in the HTML code. For instance, a script can be used to check the version of the web browser a user is running, validate input, work with applets or controls, and communicate to the user.

In addition, scripts can be used in Windows to automate operating system tasks such as changing settings or mapping a network drive.

What is a scripting engine?

The Windows Scripting Engine serves as the component within Windows that interprets and executes script code written in scripting languages such as JScript or VBScript.

What is JScript?

JScript is the Microsoft implementation of the ECMA 262 language specification (ECMAScript Edition 3).

It is an interpreted, object-based scripting language. In general, JScript has fewer capabilities than full-fledged object-oriented languages like C++. Stand-alone applications cannot be written in JScript, for example. JScript scripts can run only in the presence of an interpreter or "host", such as Active Server Pages (ASP), Internet Explorer, or Windows Script Host.

What's wrong with the Windows Script Engine for JScript?

There is a flaw in the way the JScript scripting engine processes the script. It does not correctly size a buffer during a memory operation.

Securiteam: [NT] Flaw in Windows Script Engine Could Allow Code Execution

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to cause code of the attacker's choice to run with user privileges on the system.

If I am not using Internet Explorer do I need the patch?

Yes. The vulnerability exists in the Windows Script Engine. Microsoft recommends all customers install the patch immediately.

How could an attacker exploit this vulnerability?

The attacker would need to construct a web page that contained specially formed script code. The attack could then proceed via either of two vectors. In the first, the attacker could host the web page on a web site; when a user visited the site, the web page could launch the script and exploit the vulnerability. In the second, the attacker could send the web page as an HTML mail. Upon being opened by the recipient, the web page could attempt to invoke the function and exploit the vulnerability.

In the HTML mail scenario, if the user was using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, then an attack could not be automated and the user would still need to click on a URL sent in e-mail. However if the user was not using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, the attacker could cause an attack to trigger automatically without the user having to click on a URL contained in an e-mail.

What does the patch do?

The patch addresses the vulnerability by carrying out proper input validation on the affected JScript function.

Workarounds:

Are there any workarounds that can be used to block exploitation of this vulnerability while I am testing or evaluating the patch?

Yes. Although Microsoft urges all customers to apply the patch at the earliest possible opportunity, there are a number of workarounds that can be applied to help prevent the vector used to exploit this vulnerability in the interim.

It should be noted that these workarounds should be considered temporary measures as they simply help block paths of attack rather than correcting the underlying vulnerability.

The following sections are intended to provide you with information to protect your computer from attack. Each section describes the workarounds that you may wish to use depending on your computer's configuration.

* Turn off Active Scripting support in Internet Explorer

You can turn off support for active scripting by performing the steps in the following knowledge base article:

Securiteam: [NT] Flaw in Windows Script Engine Could Allow Code Execution

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:154036>>
<http://support.microsoft.com/default.aspx?scid=kb:en-us:154036>

Note that disabling scripting support in Internet Explorer will affect the functionality of many websites on the Internet and should be considered a temporary workaround only.

* Install the Outlook Email Security Update if needed

In the case of an e-mail borne attack, if the user was using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, then an attack could not be automated and the user would still need to click on a URL sent in e-mail. However if the user was not using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, the attacker could cause an attack to trigger automatically without the user having to click on a URL contained in an e-mail. In both the web based and e-mail based cases, any limitations on the user's privileges would also restrict the capabilities of the attacker's script.

* Restrict websites to only your trusted websites

As another workaround for this issue, you can add sites that you trust to the Internet Explorer Trusted Zone, after disabling Active Scripting in the Internet Zone. This will allow you to continue using trusted web sites exactly as you do today, while tightening the restrictions on untrusted sites. When you are able to deploy the patch, you will be able to re-enable Active Scripting in the Internet Zone.

To do this, perform the following steps:

* Select "Tools," then "Internet Options." Click the "Security" tab.

* In the box labeled "Select a Web content zone to specify its current security settings," click "Trusted Sites," then click "Sites."

* If you want to add sites that don't require a secure connection, de-select the checkbox at the bottom that says "Require server verification (https:) for all sites in this zone."

* In the box labeled "Add this Web Site to the zone:," type the URL of a site that you trust, then click the "Add" button. Repeat for each site that you want to add to the zone.

* Click on OK twice to accept the changes and return to IE.

Add any sites that you trust not to take malicious action on your computer. One in particular that you may want to add is <http://windowsupdate.microsoft.com>. This is the site that hosts the patch, and it requires Active Scripting in order to install the patch. Note that there is generally a trade-off between ease-of-use and security; by selecting a high-security configuration, you could make it extremely unlikely that a malicious web site could take action against you, but at the cost of missing a lot of rich functionality. The appropriate balance between security and ease-of-use is different for everyone, and you should pick a configuration that fits your needs. The good news is that it is easy to change your configuration, and you can try different

Securiteam: [NT] Flaw in Windows Script Engine Could Allow Code Execution

configurations until you find the right one for you until you can install the patch.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_45730_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>

Microsoft Product Security.

=====

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.