

[NT] Cumulative Security Update For Internet Explorer (MS04-004)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0004.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/04/04

To: list@securiteam.com

Date: 4 Feb 2004 09:54:20 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cumulative Security Update For Internet Explorer (MS04-004)

SUMMARY

This is a cumulative update that includes the functionality of all the previously-released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0. Additionally, it eliminates the following three newly-discovered vulnerabilities:

* A vulnerability that involves the cross-domain security model of Internet Explorer. The cross domain security model of Internet Explorer keeps windows of different domains from sharing information. This vulnerability could result in the execution of a script in the Local Machine zone. To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page designed to exploit the vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e-mail message designed to exploit the vulnerability and persuade the user to view the HTML e-mail message. After the user has visited the malicious Web site or viewed the malicious HTML e-mail message an attacker who exploited this vulnerability could access information from other Web sites, access files on a user's system, and run arbitrary code on a user's system. This code would run in the security context of the currently logged on user.

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

* A vulnerability that involves performing a drag-and-drop operation with function pointers during dynamic HTML (DHTML) events in Internet Explorer. This vulnerability could allow a file to be saved in a target location on the user's system if the user clicked a link. No dialog box would request that the user approve this download. To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page that had a specially-crafted link. The attacker would then have to persuade a user to click that link. The attacker could also create an HTML e-mail message that had a specially-crafted link, and then persuade the user to view the HTML e-mail message and then click the malicious link. If the user clicked this link, code of the attacker's choice would not be executed, but could be saved on the user's computer in a targeted location.

* A vulnerability that involves the incorrect parsing of URLs that contain special characters. When combined with a misuse of the basic authentication feature that has "username:password@" at the beginning of a URL, this vulnerability could result in a misrepresentation of the URL in the address bar of an Internet Explorer window. To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page that had a specially-crafted link. The attacker would then have to persuade a user to click that link. The attacker could also create an HTML e-mail message that had a specially-crafted link, and then persuade the user to view the HTML e-mail message and then click the malicious link. If the user clicked this link, an Internet Explorer window could open with a URL of the attacker's choice in the address bar, but with content from a Web Site of the attacker's choice inside the window.

As with the previous Internet Explorer cumulative updates that were released with bulletins MS03-004, MS03-015, MS03-020, MS03-032, MS03-040, and MS03-048, this cumulative update causes the window.showHelp() control to no longer work if you have not applied the HTML Help update. If you have installed the updated HTML Help control from Microsoft Knowledge Base article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:811630>> 811630, you will still be able to use HTML Help functionality after you apply this update.

This Internet Explorer cumulative update also includes a change to the functionality of a Basic Authentication feature in Internet Explorer. The update removes support for handling user names and passwords in HTTP and HTTP with Secure Sockets Layer (SSL) or HTTPS URLs in Microsoft Internet Explorer. The following URL syntax is no longer supported in Internet Explorer or Windows Explorer after you install this software update:

`http(s)://username:password@server/resource.ext`

For more information about this change, please see Microsoft Knowledge Base article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:834489>>

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

Additionally, this update will disallow navigation to "username:password@host.com" URLs for XMLHTTP. Microsoft is currently creating an update to MSXML that will address this issue specifically for XMLHTTP and we will provide more information in this bulletin when the update becomes available.

The update also refines a change made in Internet Explorer 6 Service Pack 1, which prevents web pages in the Internet Security zone from navigating to the local computer zone. This is discussed further in the "Frequently Asked Questions" section of this bulletin.

DETAILS

Affected Components:

- * Internet Explorer 6 Service Pack 1:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=70530968-B59A-47C0-90D3-0C884910BC97&disp>
Download the update

- * Internet Explorer 6 Service Pack 1 (64-Bit Edition):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=326EFFDA-8D86-4683-BC77-9BF410BC620D&disp>
Download the update

- * Internet Explorer 6 for Windows Server 2003:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D78AE4F7-8852-4A04-B8F6-1DE327E598F0&disp>
Download the update

- * Internet Explorer 6 for Windows Server 2003 (64-Bit Edition):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6A7894F0-789F-4152-9AE4-8DCB43404149&disp>
Download the update

- * Internet Explorer 6:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=BE0C18BC-7F9A-4196-BFDE-29EBA8CF7A50&disp>
Download the update

- * Internet Explorer 5.5 Service Pack 2:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=EFFE87F6-7ACA-4A54-B767-5597DDE95C6F&disp>
Download the update

- * Internet Explorer 5.01 Service Pack 4:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=F5E74139-6E0E-49FD-9AA2-36D2D8454A92&disp>
Download the update

- * Internet Explorer 5.01 Service Pack 3:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=202D3AAC-6B56-4F4A-8C0F-4183C77B6B51&disp>
Download the update

- * Internet Explorer 5.01 Service Pack 2:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=17904608-DCEE-4C99-A780-81D6DBC48DD5&disp>
Download the update

Mitigating Factors:

There are three common mitigating factors for both the Cross Domain Vulnerability and Drag-and-Drop Operation Vulnerability:

- * By default, Internet Explorer on Windows Server 2003 runs in Enhanced Security Configuration. This default configuration of Internet Explorer blocks automatic exploitation of this attack. If Internet Explorer Enhanced Security Configuration has been disabled, the protections that are put in place that prevent these vulnerabilities from being

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

automatically exploited would be removed.

* In the Web-based attack scenario, the attacker would have to host a Web site that contains a Web page that is used to exploit these vulnerabilities. An attacker would have no way to force a user to visit a malicious Web site. Instead, the attacker would have to lure them there, typically by getting them to click a link that takes them to the attacker's site.

* By default, Outlook Express 6.0, Outlook 2002 and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed. The risk of attack from the HTML email vector can be significantly reduced if the following conditions are met:

* You have applied the update included with Microsoft Security bulletin MS03-040 or MS03-048

* You are using Internet Explorer 6 or later

* You are using the Microsoft Outlook Email Security Update or Microsoft Outlook Express 6.0 and higher, or Microsoft Outlook 2000 or later in its default configuration

* If an attacker exploited these vulnerabilities, they would gain 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 users who operate with administrative privileges.

Vulnerability identifier

* Travel Log Cross Domain Vulnerability

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1026>>
CAN-2003-1026

* Function Pointer Drag and Drop Vulnerability

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1027>>
CAN-2003-1027

* Improper URL Canonicalization Vulnerability

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1025>>
CAN-2003-1025

Workarounds

Microsoft has tested the following workarounds that apply across both the Travel Log Cross Domain Vulnerability CAN-2003-1026 and the Drag and Drop Operation Vulnerability CAN-2003-1027 the vulnerabilities. These workarounds do not mitigate the Improper URL Canonicalization Vulnerability CAN-2003-1025. These workarounds help block known attack vectors. However they will not correct the underlying vulnerabilities. Workarounds may reduce functionality in some cases; in such cases, the reduction in functionality is identified below.

Prompt before running ActiveX controls and active scripting in the Internet zone and in the Local Intranet zone

You can help protect against these vulnerabilities by changing your

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

settings for the Internet security zone to prompt before running ActiveX controls. To do this, follow these steps:

- * In Internet Explorer, click Internet Options on the Tools menu
- * Click the Security tab
- * Click Internet, and then click Custom Level
- * Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt
- * In the Scripting section, under Active Scripting, click Prompt, and then click OK
- * Click Local intranet, and then click Custom Level
- * Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt
- * In the Scripting section, under Active Scripting, click Prompt
- * Click OK two times to return to Internet Explorer

Impact of Workaround

There are side effects to prompting before running ActiveX controls. Many Web sites that are on the Internet or on an intranet use ActiveX to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX controls to provide menus, ordering forms, or even account statements. Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click Yes to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

Restrict Web sites to only your trusted Web sites

After you set Internet Explorer to require a prompt before it runs ActiveX in the Internet zone and in the Local Intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. This will allow you to continue to use trusted Web sites exactly as you do today, while helping to protect you from this attack on untrusted sites. Microsoft recommends that you only add sites that you trust to the Trusted sites zone.

- * In Internet Explorer, click Tools, click Internet Options, and then click the Security tab
- * In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites
- * If you want to add sites that do not require an encrypted channel, click to clear the Require server verification (https:) for all sites in this zone check box
- * In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add
- * Repeat these steps for each site that you want to add to the zone
- * Click OK two times to accept the changes and return to Internet Explorer

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

Add any sites that you trust not to take malicious action on your computer. One in particular that you may want to add is "*.windowsupdate.microsoft.com" (without the quotes). This is the site that will host the update, and it requires the use of an ActiveX control to install the update.

Impact of Workaround

For those sites that you have not configured to be in your Trusted sites zone, their functionality will be impaired if they require the use of ActiveX controls to function correctly. Adding sites to your Trusted sites zone will allow them to be able to download the ActiveX control that they require to function correctly. However you should only add Web sites you trust to the Trusted sites zone.

Install Outlook Email Security Update if you are using Outlook 2000 SP1 or earlier

By default, the Outlook E-mail Security Update causes Outlook 98 and 2000 to open HTML e-mail messages in the Restricted sites zone. By default, Outlook Express 6.0, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Customers who use any of these products are at reduced risk from an e-mail-borne attack that tries to exploit this vulnerability, unless the user clicks a malicious link in the e-mail message.

If you are using Outlook 2002 or Outlook Express 6.0 SP1 or later, read e-mail messages in plain text format to help protect yourself from the HTML e-mail attack vector.

Microsoft Outlook 2002 users who have applied Service Pack 1 or later and Outlook Express 6.0 users who have applied Service Pack 1 or later can enable a feature that will enable them to view all non-digitally-signed e-mail messages or non-encrypted e-mail messages in plain text only.

Digitally-signed e-mail messages and encrypted e-mail messages are not affected by the setting and may be read in their original formats.

Information about how to enable this setting in Outlook 2002 can be found in the following Knowledge Base article:

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>>
<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>

Information about how to enable this setting in Outlook Express 6.0 can be found in the following Knowledge Base article:

<<http://support.microsoft.com/?kbid=291387>>
<http://support.microsoft.com/?kbid=291387>

Impact of Workaround

E-mail that is viewed in plain text format cannot contain pictures, specialized fonts, animations, or other rich content. Additionally:

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

- * The changes are applied to the preview pane and to open messages
- * Pictures become attachments to avoid loss of message content
- * Because the message is still in Rich Text Format or in HTML format in the store, the object model (custom code solutions) may behave unexpectedly because the message is still in Rich Text Format or in HTML format in the mail store

Workarounds and other mitigations for the Improper URL Canonicalization Vulnerability

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1025>>
CAN-2003-1025 can be found in Knowledge Base article
<<http://support.microsoft.com/default.aspx?scid=kb;%5bLN%5d:833786>>
833786.

Frequently Asked Questions

Why is the update available for Windows 98, Windows 98 Second Edition, and Windows Millennium Edition (Windows Me)?

Security updates for these platforms would normally be available by request through assisted support channels, however since the issues repaired in this bulletin were reported publicly prior to this announcement the Internet Explorer 6 Service Pack 1 version of this patch will be supported on those operating systems for this release.

What vulnerabilities are eliminated by this update?

This is a cumulative update that incorporates the functionality of all previously released updates for Internet Explorer. Additionally, this update eliminates the following newly reported vulnerabilities:

- * A vulnerability that could allow an attacker to cause arbitrary code to run on the user's system
- * A vulnerability that could allow an attacker to save arbitrary code on the user's system
- * A vulnerability that could allow an attacker to mis-represent the location of a Web page in the Address bar of an Internet Explorer window

What systems are primarily at risk from the vulnerability?

Any system that has Internet Explorer installed is at risk from this vulnerability, and Microsoft recommends that this update should be installed immediately on all systems. However, these vulnerabilities require a user to be logged on and to be using Internet Explorer for any malicious action to occur. Therefore, any systems where Internet Explorer is actively used (such as user's workstations) are at the most risk from these vulnerabilities. Systems where Internet Explorer is not actively used (such as most server systems) are at a reduced risk.

Does this Security Update contain any other changes to functionality in Internet Explorer?

Yes. This Internet Explorer cumulative update also includes a change to the functionality of a Basic Authentication feature in Internet Explorer. The update removes support for handling user names and passwords in HTTP

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

and HTTP with Secure Sockets Layer (SSL) or HTTPS URLs in Microsoft Internet Explorer. The following URL syntax is no longer supported in Internet Explorer or Windows Explorer after you install this software update:

`http(s)://username:password@server/resource.ext`

For more information about this change, please see the Frequently Asked Questions section for this specific issue in this bulletin or Microsoft Knowledge Base article

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:834489>> 834489.

Additionally, this update will disallow navigation to "username:password@host.com" URLs for XMLHTTP. Microsoft is currently creating an update to MSXML that will address this issue specifically for XMLHTTP and we will provide more information in this bulletin when the update becomes available.

Does the update contain any other security changes?

The update also refines a change made in Internet Explorer 6 Service Pack 1, which prevents web pages in the Internet zone from navigating to the Local Machine zone. This change was introduced to mitigate the effects of potential new cross domain vulnerabilities. The changes introduced in this update are further enhancements of the Internet Explorer 6 Service Pack 1 restrictions.

I am running Internet Explorer on Windows Server 2003. Does this mitigate some of these vulnerabilities?

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration that mitigates both the Travel Log Cross Domain CAN-2003-1026 and the Drag and Drop Operation CAN-2003-1027 vulnerabilities. The Enhanced Security Configuration on Windows Server 2003 does not mitigate the Improper URL Canonicalization Vulnerability CAN-2003-1025.

What is Internet Explorer Enhanced Security Configuration?

Internet Explorer Enhanced Security Configuration is a group of preconfigured Internet Explorer settings that reduce the likelihood of a user or of an administrator downloading and running malicious Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying numerous security-related settings, including the settings on the Security and the Advanced tab in the Internet Options dialog box. Some of the important modifications include:

- * Security level for the Internet zone is set to High. This setting disables scripts, ActiveX controls, Microsoft Java Virtual Machine (MSJVM), HTML content, and file downloads

- * Automatic detection of intranet sites is disabled. This setting assigns all intranet Web sites and all Universal Naming Convention (UNC) paths that are not explicitly listed in the Local intranet zone to the Internet zone

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

* Install On Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running

* Multimedia content is disabled. This setting prevents music, animations, and video clips from running

Disabling Internet Explorer Enhanced Security Configuration would remove the protections that are put in place to help prevent this vulnerability from being exploited.

Is there any configuration of Windows Server 2003 that is likely to have Internet Explorer Enhanced Security Configuration disabled?

Yes. Systems Administrators who have deployed Windows Server 2003 as a Terminal Server would likely disable Internet Explorer Enhanced Security Configuration to allow users of the Terminal Server to use Internet Explorer in an unrestricted mode.

CAN-2003-1026: Travel Log Cross Domain Vulnerability Could Allow Remote Code Execution

What is the scope of this vulnerability?

This vulnerability could allow a malicious Web site operator to access information in another Internet or intranet domain or on the user's local system by injecting specially-crafted code when the browser parses specially formatted Script URLs from the travel log. This could also allow an attacker to run an executable file of their choice on the user's system.

What causes the vulnerability?

The process used to validate Script URLs in Internet Explorer's Travel Log causes this vulnerability.

What is Internet Explorer's travel log?

Internet Explorer's travel log is an interface that maintains a navigation stack for the WebBrowser control. This stack is used by Internet Explorer to maintain a list of recently visited sites. For example, the History tab in Internet Explorer is built based on information from the travel log.

What is the cross-domain security model that Internet Explorer implements?

One of the principal security functions of a browser is to make sure that browser windows that are under the control of different Web sites cannot interfere with each other or access each other's data, while allowing windows from the same site to interact with each other. To differentiate between cooperative and uncooperative browser windows, the concept of a "domain" has been created. A domain is a security boundary – any open windows within the same domain can interact with each other, but windows from different domains cannot. The cross-domain security model is the part of the security architecture that keeps windows from different domains from interfering with each other.

The simplest example of a domain is associated with Web sites. If you visit <http://www.microsoft.com>, and it opens a window to

<http://www.microsoft.com/security>, the two windows can interact with each other because both sites belong to the same domain, <http://www.microsoft.com>. However, if you visited <http://www.microsoft.com>, and it opened a window to a different Web site, the cross-domain security model would protect the two windows from each other. The concept goes even further. The file system on your local computer is also a domain. For example, <http://www.microsoft.com> could open a window and show you a file on your hard disk. However, because your local file system is in a different domain from the Web site, the cross-domain security model should prevent the Web site from reading the file that is being displayed.

The Internet Explorer cross-domain security model can be configured by using the security zone settings in Internet Explorer.

What are Internet Explorer security zones?

Internet Explorer security zones are a system that divides online content into categories or zones based on its trustworthiness. Specific Web domains can be assigned to a zone, depending on how much trust is placed in the content of each domain. The zone then restricts the capabilities of the Web content, based on the zone's policy. By default, most Internet domains are treated as part of the Internet zone, which has default policy that prevents scripts and other active code from accessing resources on the local system.

What is the issue with the way Internet Explorer calculates cross domain security?

Internet Explorer evaluates security when one Web Page requests access to resources in another security zone. However, there is a vulnerability in the process used to calculate security when specially formatted Script URLs are parsed out of the Travel Log. As a result, an attacker can bypass the security checks.

What could this vulnerability enable an attacker to do?

An attacker could use this vulnerability to create a Web page that could allow the attacker to access data across domains. This could include accessing information from other Web sites, from local files on the system, or from running executable files that already exist on the local file system. This could also include running executable files of the attacker's choice on the user's local file system.

How could an attacker exploit this vulnerability?

An attacker could exploit this vulnerability by creating a malicious Web page or an HTML e-mail message and then enticing the user to visit this page or to view the HTML e-mail message. When the user visited the page or viewed the e-mail message, the attacker could access information from other websites, local files on the system, or cause script to run in the security context of the Local Machine Zone.

What does the update do?

The update addresses the vulnerability by ensuring that cross domain

security checks take place whenever Script URLs are parsed from the Travel Log.

CAN-2003-1027: Function Pointer Drag and Drop Operation Vulnerability Could Allow Arbitrary Code to be Saved on User's System

What is the scope of the vulnerability?

This vulnerability involves using a drag and drop event in Internet Explorer with function pointers and could result in a file being saved on the user's system when the user clicked a link (the user would not receive a dialog box requesting to approve the download). To exploit this vulnerability, an attacker would have to host a malicious Web site or create an HTML e-mail that contained a link that is designed to exploit this particular vulnerability and then persuade a user to visit that site. If the user visited the page or viewed the e-mail message, and if the user clicked the malicious link, then code of the attacker's choice could be saved in a targeted location on the user's computer.

What causes the vulnerability?

The process by which the drag and drop technology validates certain Dynamic HTML (DHTML) events causes this vulnerability. As a result, a file could be downloaded to the user's system after the user clicks a link.

What are DHTML events?

DHTML events are special actions that are provided by the DHTML Object Model. These events can be used in script code to add dynamic content to a Web site.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could save code of their choice to the user's local file system. Although this code could not be executed through this vulnerability directly, the operating system might open the file if it is dropped to a sensitive location, or a user may click the file inadvertently, causing the attacker's code to be executed.

How could an attacker exploit this vulnerability?

To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page or an HTML e-mail with a link that is designed to exploit this particular vulnerability and then persuade a user to visit that site. If the user clicked the malicious link, any code of the attacker's choice could be saved on the user's computer in a targeted location.

What systems are primarily at risk from the vulnerability?

Any system that has Internet Explorer installed is at risk from this vulnerability, and this update should be installed immediately on all systems. However, this vulnerability requires a user to be logged on and to be using Internet Explorer for any malicious action to occur. Therefore, any systems where Internet Explorer is actively used (such as user's workstations) are at the most risk from this vulnerability. Systems where Internet Explorer is not actively used (such as most server systems)

are a reduced risk.

What does the update do?

This update corrects this vulnerability by correctly evaluating drag-and-drop operations by using function pointers during DHTML events.

CAN-2003-1025: Improper URL Canonicalization Vulnerability Could Allow Attacker to Spoof Websites

What's the scope of the vulnerability?

There is a vulnerability that involves the address bar that is used by Internet Explorer to display the currently visited Web site. This vulnerability could result in an incorrect URL being listed in the Address bar that is not the actual Web page that is displayed by Internet Explorer.

What causes the vulnerability?

This vulnerability is caused by a canonicalization error that occurs when Internet Explorer parses special characters in a HTTP URL.

What is an HTTP URL?

An HTTP URL is a Uniform Resource Locator used to designate an address to a resource reachable via the HTTP protocol. While the generic syntax for a URIs is defined in <http://www.ietf.org/rfc/rfc2396.txt> RFC 2396 – Uniform Resource Identifiers (URI): Generic Syntax, the specific syntax for a HTTP URL is defined in <http://www.w3.org/Protocols/rfc2616/rfc2616.html> RFC 2616 – Hypertext Transfer Protocol -- HTTP/1.1:

```
http_URL = "http:" "/" host [ ":" port ] [ abs_path [ "?" query ] ]
```

What might an attacker use the vulnerability to do?

An attacker could use this vulnerability to create a Web Page that would display a URL of the attackers choosing in the address bar, while displaying a different Web Site in the browser window. An attacker could use this vulnerability to create a malicious page that spoofs a legitimate site. For example an attacker could create a Web Page that looks like a user's on-line E-mail site. While this Web Page would be hosted on a malicious Web Site, an attacker could use this vulnerability to display a legitimate looking URL in the address bar. A user might see this URL and mistakenly give away sensitive information to the attacker's site.

How could an attacker exploit this vulnerability?

To exploit one of this vulnerability, an attacker would have to host a malicious Web site that contains a Web page that has a specially-crafted link. The attacker would then have to persuade a user to click that link. The attacker could also create an HTML e-mail message that has a specially-crafted link, and then persuade the user to view the HTML e-mail message and then click the malicious link. If the user clicked this link, an Internet Explorer window could open with an HTTP URL of the attacker's choice in the Address bar, but with content from a Web site of the attacker's choice.

Securiteam: [NT] Cumulative Security Update For Internet Explorer (MS04-004)

What does the update do?

The update corrects the vulnerability by making sure that Internet Explorer correctly parses special characters in URLs to make sure that the correct address is represented in the Address bar. This update also makes Internet Explorer's handling of HTTP URLs more compliant with RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1 by removing the ability to perform basic authentication by using a "username:password@" format. This change to the default behavior of Internet Explorer is discussed further in Knowledge Base article [834489](http://www.support.microsoft.com/default.aspx?scid=kb;%5bLN%5d:834489).

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security
The original article can be found at:
<http://www.microsoft.com/technet/security/bulletin/winfeb04.asp>

=====
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.