

[NT] Dotless IP Addresses Can Cause IE to Move into Intranet Zone

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0046.html>

From: support@securiteam.com

Date: 10/17/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Dotless IP Addresses Can Cause IE to Move into Intranet Zone

Message-Id: <20011017204447.A7760138C4@mail.der-keiler.de>

Date: Wed, 17 Oct 2001 22:44:47 +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.

Dotless IP Addresses Can Cause IE to Move into Intranet Zone

SUMMARY

Microsoft has released a patch that eliminates three vulnerabilities affecting Internet Explorer. The first involves how IE handles URLs that include dotless IP addresses. If a web site were specified using a dotless IP format (e.g., <http://031713501415> rather than <http://207.46.131.13>), and the request were malformed in a particular way, IE would not recognize that the site was an Internet site. Instead, it would treat the site as an intranet site, and open pages on the site in the Intranet Zone rather than the correct zone. This would allow the site to run with fewer security restrictions than appropriate. This vulnerability does not affect IE 6.

The second involves how IE handles URLs that specify third-party sites. By encoding an URL in a particular way, it would be possible for an attacker to include HTTP requests that would be sent to the site as soon as a connection had been established. These requests would appear to have originated from the user. In most cases, this would only allow the attacker to send the user to a site and request a page on it. However, if exploited against a web-based service (e.g., a web-based mail service), it could be possible for the attacker to take action on the user's behalf,

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

including sending a request to delete data.

The third is a new variant of a vulnerability discussed in Microsoft Security Bulletin MS01-015, affecting how Telnet sessions are invoked via IE. By design, telnet sessions can be launched via IE. However, a vulnerability exists because when doing so, IE will start Telnet using any command-line options the web site specifies. This only becomes a concern when using the version of the Telnet client that installs as part of Services for Unix (SFU) 2.0 on Windows NT 4.0 or Windows 2000 machines. The version of the Telnet client in SFU 2.0 provides an option for creating a verbatim transcript of a Telnet session. An attacker could start a session using the logging option, then stream an executable file onto the user's system in a location that would cause it to be executed automatically the next time the user booted the machine. The flaw does not lie in the Telnet client, but in IE, which should not allow Telnet to be started remotely with command-line arguments.

DETAILS

Vulnerable systems:

- * Microsoft Internet Explorer 5.01
- * Microsoft Internet Explorer 5.5
- * Microsoft Internet Explorer 6

Mitigating factors:

Zone spoofing vulnerability:

* The default settings in the Intranet Zone differ in only a few ways from those of the Internet Zone. The differences are enumerated in the FAQ, but none would allow destructive action to be taken.

HTTP request encoding vulnerability:

* In order to exploit this vulnerability successfully, the attacker would need to possess significant personal information about the victim, such as what web services the user subscribed to, folder structures, and so forth.

* Even if the attacker knew the requisite personal information, factors outside of the attacker's control (such as whether the user was logged onto the service already) could cause the user to see prompts and dialogues that would indicate that an attack was underway.

* It is unlikely that the vulnerability could be used to target large populations; it is likely that it could be used only against specific targets.

New variant of telnet invocation vulnerability:

* This vulnerability is only a concern for customers who are using the Telnet client that ships as part of Services for Unix 2.0. No other versions of Telnet contain the command-line feature to create log files, including the versions that ship by default as part of Windows platforms.

Patch availability:

Download locations for this patch

<http://www.microsoft.com/windows/ie/downloads/critical/q306121/default.asp>
<http://www.microsoft.com/windows/ie/downloads/critical/q306121/default.asp>

What are the vulnerabilities discussed in this bulletin?

What are the vulnerabilities discussed in this bulletin? This bulletin discusses three vulnerabilities:

- * A vulnerability that could enable a web site to render with less-restrictive security settings than are appropriate.
- * A vulnerability that could enable an attacker to send a user to a third-party web site and send commands to it in the guise of the user.
- * A new variant of a previously reported vulnerability that could enable an attacker to write files onto a user's computer via Telnet.

What's the scope of the first vulnerability?

This vulnerability could allow a web site to take actions that it should not be able to take on visiting users' systems. Specifically, it could allow the web site to trick IE into treating it as though it was located on the user's intranet, thereby gaining the ability to use less-restrictive security settings than are appropriate. A user could be affected by this vulnerability by either surfing to an attacker's web site or opening an HTML mail from an attacker.

If the security settings were left in their defaults, the additional privileges the web site would gain still would not allow it to take any destructive action. The greater danger from this vulnerability would arise in the case where the user had give intranet sites additional latitude. IE 6 is not affected by the vulnerability.

What causes the vulnerability?

The vulnerability results because it is possible to refer to a web using a particular type of dotless IP address, with the result that IE handles the site in the Local Intranet Zone rather than the correct one.

What's a dotless IP address?

Internet addresses are typically provided using a "dotted" address format. For instance, the address of the Microsoft web site in dotted format is <http://207.46.131.13>. However, it is possible to use other formats. For instance, you could also use a "dotless" format, in which the bit sequence corresponding to the dotted address is treated as a numerical value. For instance, the Microsoft web site's address could be rendered as <http://031713501415>. These are equivalent representations, and both are valid ways to refer to the web site.

A vulnerability occurs because, if an Internet address is provided in dotless form and is malformed in particular way, IE uses the wrong Security Zone to process the web pages at the site.

What are Security Zones?

Security Zones are a feature in Internet Explorer that lets you regulate what actions web sites can take on your computer. All web content is

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

categorized into one of five Security Zones:

- * The Restricted Sites Zone, which contains any sites you have designated as being untrustworthy.
- * The Trusted Sites Zone, which contains any sites you have designated as being trustworthy.
- * The Internet Zone, which contains all Internet sites that are not in either the Restricted Sites or Trusted Sites zones.
- * The Intranet Zone, which contains all web sites within a local intranet. You can't add sites to this zone; instead, IE determines whether a site belongs in this zone by its IP address
- * The Local Computer Zone, which contains all web content on your computer. Like the * Intranet Zone, you cannot add sites to this zone; IE determines whether content is on the local computer or not.

Each zone has a set of security settings associated with it, and these determine the latitudes that sites in that zone will be given. In addition, the security settings for each zone can be customized according to the user's preferences.

What's wrong with the way IE handles zone information?

If a web site's Internet address is provided using an unusual variation of a dotless IP address, IE will treat the site as though it was in the Intranet Zone rather than the zone it actually belongs to. This would allow the site to operate with the less-restrictive security settings of the Intranet Zone.

What could an attacker do using this vulnerability?

An attacker could exploit this vulnerability to make a web site on the Internet render using the lowered security settings associated with the Intranet zone. The specific actions the web site could take would vary, depending on whether the user had customized the security settings in the Intranet Zone. The default settings would not allow any destructive action; however, many users customize the Intranet Zone and give intranet sites considerable latitude.

What are the differences between the default settings for the Intranet Zone and the Internet Zone?

Here are the settings that differ by default in the two zones:

- * Java permissions. This setting defaults to "medium" in the Intranet Zone, but "high" in the Internet Zone
- * Access data sources across domains. This is set to "prompt" in the Intranet Zone, but "disable" in the Internet zone.
- * Don't prompt for certificate selection when no certificate or only one certificate exists. This is set to "enable" in the Intranet Zone, but "disable" in the Internet Zone.

How might an attacker exploit the vulnerability?

There are two ways the attacker might try to exploit the vulnerability:

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

* By persuading or coercing a user into visiting a web site that uses the vulnerability to open one of its pages in the Intranet Zone.

* By sending an HTML mail to the user that, when opened, would open a web page in the Intranet Zone

Could this vulnerability be exploited accidentally?

No. Few sites actually use dotless IP addressing, and it would be very unlikely for even such a site to use the specific type of malformed dotless IP addressing at issue here.

Does this vulnerability affect IE 6?

No. However, IE 6 customers should consider applying the patch anyway, as it also eliminates two vulnerabilities that do affect IE 6.

What does the patch do?

The patch eliminates the vulnerability by causing IE to correctly identify a web site's Zone, even if it uses the form of dotless IP addressing discussed here.

What's the scope of the second vulnerability?

This vulnerability could enable an attacker to send a user to third-party site, and include commands that, to the third-party site, would appear to have come from the user. The precise actions that could be taken via these commands would vary from site to site, but one example of a potential action would be to send a user to her web-base mail service with a command to delete her mail.

It is unlikely that this vulnerability could be used in any widespread attack, as exploiting it would require detailed knowledge of the web services the user uses, and would likely require information that was specific to the user. However, it could be damaging if targeted against a selected user.

What causes the vulnerability?

The vulnerability results because it is possible to create an URL that specifies the domain name of a third-party site and a series of HTTP requests. Upon processing such an URL, IE would establish a connection with the third-party site, and then send the commands as though they had originated from the user.

What are HTTP requests?

HTTP (Hypertext Transfer Protocol) is the industry-standard protocol by which data is exchanged between web sites and machines that visit them. HTTP requests are commands to a web server – to, for instance, request a web page or ask the server to take some action for the visiting user.

What's wrong with the way IE handles HTTP requests?

The problem in this case is that if a reference to a web site were coded in a particular way, IE could be made to send one or more HTTP requests to the site as soon as the connection were established.

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

How could an attacker exploit this vulnerability?

An attacker could embed a link in either a web page or an HTML mail that, when clicked, would take the user to a site of the attacker's choosing and send commands to it in the guise of the user.

What would this enable an attacker to do?

In most cases, it would allow the attacker to do very little. Most web sites only serve content. Exploiting this vulnerability in such a case would only allow the attacker to send the user to a particular site and request a particular page.

However, the situation could be different if the user subscribed to a web-based service of some kind, such as a web-based email service. In such a case, it could be possible for the attacker to encode commands that would, for instance, delete the user's mail. However, such an attack would likely be difficult to carry out.

Why would it be difficult to carry out such an attack?

First, it would require a great deal of specific knowledge about the victim. For instance, consider what would be required in order to delete a user's mail on a web-based mail service. The attacker would need to know what mail service the user subscribed to, and might possibly need to know the server name. The attacker also might need to know details such as the names of the user's mail folders.

Second, unless the timing was precise, the user might be presented with dialogues and other information that would serve as a clue that something was amiss. Again considering a case in which the attacker wanted to delete another user's mail, it's likely that the user, unless already logged into the service at the time, would see a login prompt. Also, depending on the mail service, the user might get a confirmation prompt before the folders would be deleted.

Does this mean the vulnerability doesn't pose a risk?

No. What this means is that it's unlikely that this vulnerability could be used to attack a large population of users. However, an attacker who was targeting one particular person might be able to use it effectively.

What does the patch do?

The patch prevents HTTP requests from being appended to domain names in URLs.

What's the scope of the new variant of the Telnet vulnerability?

It's exactly the same as the original variant, which we discussed in Microsoft Security Bulletin

<http://www.securiteam.com/windowsntfocus/5IP012A3PQ.html> MS01-015, and could enable an attacker to write files onto the system of a user who either visited the attacker's web site, or who opened a specially-formatted HTML mail the attacker sent. The attacker could use the vulnerability to carry out a variety of attacks, the most serious of which would enable him to place a program onto the user's system, which

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

could then be made to run automatically each time the user logged on.

As in the original variant, the vulnerability could only be exploited if a particular version of the Telnet utility were installed on the system. This version is only available as part of a separate add-on package that can only be installed on Windows NT 4.0 and Windows 2000 systems. It does not ship by default as part of any platform.

Are there any differences at all between the original variant and the new one?

The only difference lies in the specific Telnet option that the attacker might use to exploit the vulnerability. In all other respects, this is exactly the same vulnerability as the one we discussed in MS01-015.

Security Bulletin MS01-015 says that this only affects customers who are using the Telnet client in Services for Unix 2.0. Is this also true of the new variant?

Yes. You could only be affected by this vulnerability if you've loaded the Telnet client from the Services for Unix 2.0 add-on package. If you are using the default Telnet client, you cannot be affected by the vulnerability.

Does the new patch eliminate both the new and original variants of the vulnerability?

No. However, the versions of IE that the patch can be installed on (IE 5.01 SP2, IE 5.5 SP2, and IE 6) already contain the fix for the original variant. As a result, if you apply the patch, you're fully protected against all variants of the vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@kikkert.nl> Michiel Kikkert, <mailto:tharbad@kaotik.org> Joao Gouveia, and <mailto:secnotif@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.

Securiteam: [NT] Dotless IP Addresses Can Cause IE to Move into

- **Previous message:** support@securiteam.com: "[\[UNIX\] Security Bug Found in ht://Dig htsearch CGI \(DoS, File Exposure\)](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)