

[NT] Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/17/03

To: list@securiteam.com

Date: 17 Jul 2003 11:24:26 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

SUMMARY

ISA Server contains a number of HTML-based error pages that allow the server to respond to a client requesting a Web resource with a customized error. A cross-site scripting vulnerability exists in many of the error pages that are returned by ISA Server under specific error conditions.

To exploit this flaw, an attacker would have to first be aware of a specific ISA server and its access policies or host an ISA server of their own and create specific access policies designed to exploit this vulnerability. The attacker could then construct a request to trigger a page refusal. Once the attack was crafted, the attacker would have to host a Web site containing the link, or send the link to the user in the form of an HTML e-mail. After the user previewed or opened the e-mail, the malicious site could be visited automatically without further user interaction. In the Web-based attack scenario, an attacker would have no way to force a user to visit the Web site.

Securiteam: [NT] Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

DETAILS

Affected Software:

- * Microsoft Internet Security and Acceleration (ISA) Server 2000

Mitigating factors:

* The vulnerability could only be exploited if the attacker could entice another user into visiting a Web page, or opening an HTML-based e-mail.

* The request must be one that would cause the ISA server to respond with one of several affected error pages.

* The vulnerability would not normally enable an attacker to gain any privileges on an affected ISA Server computer, breach the firewall, or compromise any cached content, unless the user is operating on the ISA server itself and is using the Web Proxy service to access the Internet.

Patch availability:

Download locations for this patch

- * Microsoft ISA Server:

English –

<<http://download.microsoft.com/download/4/6/4/464c95cd-8488-410d-bacb-69b25eaa7822/ISA2000-KB816456-x86-ENU-ENU.exe>>
<http://download.microsoft.com/download/4/6/4/464c95cd-8488-410d-bacb-69b25eaa7822/ISA2000-KB816456-x86-ENU-ENU.exe>

French –

<<http://download.microsoft.com/download/a/d/6/ad64a2af-d359-44e5-88d9-321269f1afde/ISA2000-KB816456-x86-FRA-FRA.exe>>
<http://download.microsoft.com/download/a/d/6/ad64a2af-d359-44e5-88d9-321269f1afde/ISA2000-KB816456-x86-FRA-FRA.exe>

German –

<<http://download.microsoft.com/download/9/f/3/9f39d8a7-4897-43e5-bd90-70cc468139ae/ISA2000-KB816456-x86-DEU-DEU.exe>>
<http://download.microsoft.com/download/9/f/3/9f39d8a7-4897-43e5-bd90-70cc468139ae/ISA2000-KB816456-x86-DEU-DEU.exe>

Spanish –

<<http://download.microsoft.com/download/5/a/a/5aabcffe-e89c-4275-b2ba-64c47e42f078/ISA2000-KB816456-x86-ESP-ESP.exe>>
<http://download.microsoft.com/download/5/a/a/5aabcffe-e89c-4275-b2ba-64c47e42f078/ISA2000-KB816456-x86-ESP-ESP.exe>

Japanese –

<<http://download.microsoft.com/download/1/5/b/15b400a5-5b40-4721-92b0-caef3f190146/ISA2000-KB816456-x86-JPN-JPN.exe>>
<http://download.microsoft.com/download/1/5/b/15b400a5-5b40-4721-92b0-caef3f190146/ISA2000-KB816456-x86-JPN-JPN.exe>

What's the scope of the vulnerability?

This is a cross-site scripting (XSS) vulnerability that could allow an attacker to construct a request to an affected server that would cause a Web page containing script to be sent to another user. The script would execute within the user's browser as though it had come from the third-party site. This would let it run using the security settings appropriate to the third-party Web site, as well as allowing the attacker to access any data belonging to the site. The vulnerability could only be exploited if the user opened an HTML-based e-mail or clicked a specially crafted link.

What's cross-site scripting?

Cross-site scripting (XSS) is a security vulnerability that potentially enables a malicious user to "inject" code into a user's session with a Web site. Unlike most security vulnerabilities, XSS does not apply to any

Securiteam: [NT] Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

single vendor's products – instead, it can affect any software that runs on a Web server and that does not follow defensive programming practices.

How does XSS work?

At a high level of detail, here is how XSS works. Suppose that Web site A offers a search feature that lets a user type a word or phrase to search for. If the user typed "banana" in as the search phrase, the site would search for the phrase and then generate a Web page saying, "I'm sorry, but I can't find the word 'banana'.". It would send the Web page to the user's browser, which would then parse the page and display it. Now suppose that, instead of typing "banana" as the search phrase, the user typed something like "banana < SCRIPT> Alert('Hello'); </SCRIPT>". If the search feature were written to blindly use whatever search phrase it's provided, it would search for the entire string and create a Web page saying "I'm sorry, but I can't find the word "banana < SCRIPT> Alert('Hello'); </SCRIPT>"". However, all of the text beginning with "< SCRIPT>" and ending with "</SCRIPT>" is actually program code, so when the page was processed, a dialog box that says "Hello" would appear by the user's browser.

So far, this example has only shown how a user could "relay" code off a Web server and make it run on his own computer. This is not a security vulnerability. However, it's possible for a malicious Web site operator to invoke this vulnerability to run on the computer of a user who visits his site. If Web site B were operated by a malicious user who was able to entice the user into visiting it and clicking a hyperlink, Web site B could go to Web site A, fill in the search page with malicious script, and submit it on behalf of the user. The resulting page would return to the user (because the user, having clicked on the hyperlink, was ultimately the requester), and process on the user's computer.

What could the script do on the user's machine? In the security context of Web site A?

The script from Web site B (the attacker's site) would run on the user's computer as though it had come from Web site A. In practical terms, this would mean that it would run using the security settings on the user's machine that were appropriate to Web site A.

The script from Web site B would be able to access cookies and any other data on the user's system that belonged to Web site A.

What is ISA Server?

ISA Server provides both an enterprise firewall and a high-performance Web cache. The firewall protects the network by regulating which resources can be accessed through the firewall, and under what conditions. The Web cache helps improve network performance by storing local copies of frequently requested Web content. ISA Server can be installed in three modes: firewall mode, cache mode, or integrated mode.

Could an attacker use the vulnerability to take control of an ISA Server computer?

No. This is a cross-site scripting attack only. There is no capability to

Securiteam: [NT] Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

usurp any administrative privileges on the ISA Server.

Could an attacker use the vulnerability to breach the security of the firewall?

No. There is no capability to use this vulnerability to lower the security the firewall provides to the network. Firewall mode allows an administrator to secure network communication by configuring rules that control communication between the corporate network and the Internet. Cache mode improves network performance by storing frequently accessed Web pages on the server itself. In integrated mode, all cache and firewall features are available.

What causes the vulnerability?

The vulnerability results because some of the error pages returned by ISA Server display the requested URL in HTML text without proper encoding.

What's wrong with ISA Server error pages?

The homepage() function in many of the ISA error pages does not correctly encode the URL for displaying in HTML text. As a result, it is possible to embed a link to script on a separate Web site and cause this to be returned to the Web browser.

What would this vulnerability enable an attacker to do?

The vulnerability would allow an attacker who operated a Web site and was able to lure another user into clicking a link on it to carry out a cross-site scripting attack via another Web site that was running through ISA Server. This would enable the attacker to run script in the user's browser using the security settings of the other Web site, and to access cookies and other data belonging to it.

How could an attacker exploit this vulnerability?

To exploit this flaw, an attacker would have to first be aware of a specific ISA server and its access policies, or host an ISA server of their own and create specific access policies designed to exploit this vulnerability. The attacker could then construct a request to trigger a page refusal. Once the attack was crafted, the attacker would have to host a Web site containing the link or send the link to the user in the form of an HTML e-mail. After the user previewed or opened the e-mail, the malicious site could be visited automatically without further user interaction. In the Web-based attack scenario, an attacker would have no way to force a user to visit the Web site.

You said that the point of the attack would be for the attacker to get script running in the user's browser using the security settings of my Web site. What specific capabilities would the attacker gain by doing this?

It would vary from site to site, based on what Security zone the attacker's site and yours were placed in.

If they were both in the same zone (and, by default, all Web sites reside in the Internet zone unless the user moves them), they would both be subject to exactly the same security restrictions, and the attacker would

Securiteam: [NT] Flaw in ISA Server Error Pages Could Allow Cross-Site Scripting Attack

gain different abilities through the vulnerability. For instance, an attacker could affect the relationship between a user and their Web-based e-mail.

If the user had put the attacker's site into a more restricted zone than yours, the attacker would gain the ability for his script to do anything on the user's computer that script from your site could do.

If the user had put your site into a more restricted zone than yours, the attacker would actually lose capabilities through the attack.

It's important to note, however, that regardless of the security settings, the attacker's script would always be able to access cookies and any other data on the user's system belonging to the third-party site. This is because, as far as the browser can tell, the attacker is the third-party site.

How does the patch eliminate the vulnerability?

The patch eliminates the vulnerability by removing the homepage() functionality as well as the JavaScript command for refreshing the page and for navigating back.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_50146_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.