

[NT] Cross Site Scripting and Memory Leak Vulnerabilities in ISA Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0075.html>

From: support@securiteam.com

Date: 08/19/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Cross Site Scripting and Memory Leak Vulnerabilities in ISA Server

Message-Id: <20010819062156.8E81C138BF@mail.der-keiler.de>

Date: Sun, 19 Aug 2001 08:21:56 +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.

Cross Site Scripting and Memory Leak Vulnerabilities in ISA Server

SUMMARY

This bulletin discusses three security vulnerabilities that are unrelated except in the sense that all affect ISA Server 2000:

* A denial of service vulnerability involving the H.323 Gatekeeper Service, a service that supports the transmission of voice-over-IP traffic through the firewall. The service contains a memory leak that is triggered by a particular type of malformed H.323 data. Each time such data is received, the memory available on the server is depleted by a small amount; if an attacker repeatedly sent such data, the performance of the server could deteriorate to the point where it would effectively disrupt all communications across the firewall. A server administrator could restore normal service by cycling the H.323 service.

* A denial of service vulnerability in the in the Proxy service. Like the vulnerability above, this one is caused by a memory leak, and could be used to degrade the performance of the server to point where communications are disrupted.

* A cross-site scripting vulnerability affecting the error page that ISA Server 2000 generates in response to a failed request for a web page. An attacker could exploit the vulnerability by tricking a user into

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

submitting to ISA Server 2000 an URL that has the following characteristics: (a) it references a valid web site; (b) it requests a page within that site that can't be retrieved – that is, a non-existent page or one that generates an error; and (c) it contains script within the URL. The error page generated by ISA Server 2000 would contain the embedded script commands, which would execute when the page was displayed in the user's browser. The script would run in the security domain of the web site referenced in the URL, and would be able to access any cookies that site has written to the user's machine.

DETAILS

Affected software:

- * Microsoft ISA Server 2000

Mitigating factors:

H.323 Denial of service vulnerability:

- * The vulnerability could only be exploited if the H.323 Gatekeeper Service was installed. It is only installed by default if "Full Installation" is chosen; if "Typical Installation" is selected, it is not installed.

- * The vulnerability would not enable an attacker to gain any privileges on an affected server or add any traffic to an existing voice-over-IP session. It is strictly a denial of service vulnerability.

Proxy Service Denial of service vulnerability:

- * The vulnerability could only be exploited by an internal user; it could not be exploited by an Internet user.

- * The vulnerability would not enable an attacker to gain any privileges on an affected server or compromise any cached content on the server. It is strictly a denial of service vulnerability.

Cross-site scripting vulnerability:

- * In order to run script in the security domain of a trusted site, the attacker would need to know which sites, if any, a user trusted. Most users use the default security settings for all web sites, which would effectively deny an attacker any gain in exploiting the vulnerability for the purposes of running script.

- * An attacker who wished to read other sites' cookies on a user's machine would have no way to know which sites had placed cookies there. The attacker would need to exploit the vulnerability once for every web site whose cookies she wished to access.

- * Even if the attacker correctly guessed which sites had placed cookies on a user's machine, there should be no sensitive information in the cookies, if best practices have been followed.

Patch availability:

Download locations for this patch

- * Microsoft ISA Server 2000:

<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32094>>
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32094>

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

What vulnerabilities are discussed in this bulletin?

This bulletin discusses three unrelated vulnerabilities affecting ISA Server 2000:

- * A vulnerability that could enable an attacker to disrupt service on an ISA server via an Internet Telephony service.
- * A vulnerability that could enable an attacker to disrupt service on an ISA server via the Web Proxy Service.
- * A vulnerability that could enable an attacker under very unusual conditions to take action or view cookies on a user's computer.

What is the scope of the first vulnerability?

The first vulnerability is a denial of service vulnerability. By repeatedly sending a particular type of malformed data, an attacker could degrade the performance of an affected ISA server, potentially to the point of disrupting communications across the server. Depending on where the server was located within the network, this could cause parts of the network to be isolated from each other, or for users inside the network to be unable to reach the Internet.

The vulnerability only occurs if a particular service supporting IP telephony is enabled. This service is not installed by default in typical installations.

What causes the vulnerability?

The vulnerability results because of a memory leak in the H.323 Gatekeeper Service in ISA Server.

What is the H.323 Gatekeeper Service?

H.323 is an international telephony standard that specifies how voice communications over media like the Internet should be handled. The H.323 Gatekeeper Service in ISA Server implements this standard, and allows voice-over-IP communications to pass through the firewall.

What is a memory leak?

A memory leak is an implementation error that depletes the available memory on a system. As a process on a computer runs, it may need more or less memory, depending on exactly what it is doing from one minute to the next. When the process needs more memory, it requests it from the operating system; when it no longer needs the additional memory, it should return it to the operating system so it can be allocated to other processes.

If a process does not correctly return memory to the operating system, the memory remains assigned to the process even though the process is no longer using it, and the memory cannot be re-allocated. This effectively makes the block of memory unavailable. In this case, the H.323 Gatekeeper Service has an implementation error that results in a memory leak when certain invalid data is sent to it.

What could an attacker do via this vulnerability?

An attacker could deliberately send a large number of the malformed H.323

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

data in order to deplete the server's available memory. As the attack continued and the pool of memory on the server was depleted, the server's performance would gradually slow, potentially to the point where it no longer provided any service at all.

Do you mean that a successful attack would prevent the H.323 service from performing useful work, or the entire ISA server?

The memory leak affects the pool of memory used by all software on the system, so a successful attack would affect the server as a whole.

What would be the effect of disrupting service on the system?

ISA Server can be configured to act as a firewall, a web proxy, or both. In either role, ISA serves as a communication conduit between parts of a network, or between the network and the Internet. If the H.323 Gatekeeper Service was attacked via this vulnerability, the effect would be to slow those communications or potentially block them altogether.

How could an affected server be put back into service?

The server administrator could restore normal service by stopping and starting ISA Server 2000.

Could this vulnerability be exploited from the Internet?

Yes. Both internal and external users can send data to the H.323 Gatekeeper Service.

Suppose the H.323 Gatekeeper Server was disabled. Could the vulnerability be exploited then?

No. The vulnerability only affects ISA servers that have the H.323 Gatekeeper Service enabled. The service is installed by default if "Full Installation" is chosen when installing ISA Server 2000; however, if "Typical Installation" is chosen, the H.323 Gatekeeper Service is not installed.

Does the vulnerability provide any way for an attacker to gain control over the server, or undermine the security of the firewall?

No. It could be used to gain any privileges on server. It could only be used to deny services to legitimate users.

Does the vulnerability provide any way for an attacker to eavesdrop on a voice-over-IP session, or to add bogus data to it?

No. It does not provide any way for an attacker to break into an existing H.323 session.

What does the patch do?

The patch causes the H.323 Gatekeeper Service to correctly allocate and deallocate memory, thereby removing the memory leak.

What is the scope of the second vulnerability?

This vulnerability is virtually identical to the first vulnerability above. Like that vulnerability, this one could be used to degrade the performance of a system running ISA Server 2000, potentially to the point

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

where communications between the internal and external network would be disrupted. The seriousness of this vulnerability is mitigated somewhat by the fact that it could only be exploited from within a network.

What causes the vulnerability?

Like the vulnerability above, this one results because of a memory leak. In this case, the leak is in the Proxy Service of ISA Server 2000.

What would the effect of exploiting this vulnerability be?

As in the case above, this vulnerability could enable an attacker to degrade the performance of an ISA Server, potentially to the point of disrupting communications across the proxy server.

Are there any differences between the two vulnerabilities?

Yes. Unlike the memory leak in the H.323 Gatekeeper Service, the one in the Proxy Service could only be exploited from within the network. That is, it would not be possible for an attacker on the Internet to exploit the vulnerability.

Is the Proxy Service installed by default?

Yes.

What does the patch do?

The patch causes the Proxy Service to correctly allocate and deallocate memory.

What is the scope of the third vulnerability?

This vulnerability could enable an attacker to perform either of two actions:

- * Cause web content to execute with the security settings appropriate to a trusted web site.
- * Read cookies set by a trusted web site.

In practice, however, exploiting this vulnerability would be a daunting challenge. The attacker would likely have no way to know which web sites, if any, a particular user trusted. Likewise, if best practices have been followed and a site's cookies do not contain any sensitive information, gaining the ability to read them would not represent any gain for the attacker.

What causes the vulnerability?

The vulnerability results because an error message – specifically, the one ISA Server generates when it cannot retrieve a requested web page – is susceptible to cross-site scripting.

What is cross-site scripting?

Cross-site scripting is a type of security vulnerability that results when web content does not adequately filter its inputs. In most cases, cross-site scripting occurs when a web page accepts some kind of user input (e.g., a phrase to search for) and then creates a page using that input. If the page does not check for the presence of script within the

user's input, the result is that the script, when processed as part of the web page, will run within the web site's domain.

Such a condition is not dangerous in the case in which the user provides the input – after all, the user could have performed the actions directly rather than performing them via the script. However, as discussed in the Cross-site Scripting FAQ, there are cases in which it is possible for a third party to "inject" inputs containing script into a user's web session. This does pose a hazard, because it could enable the third party's script to run in the user's browser using the security settings appropriate to the web page.

What can be done via cross-site scripting?

Cross-site scripting offers two possibilities for an attacker:

- * Running script in the security settings of another, presumably trusted, web site. For instance, suppose John trusted Web Site A and had relaxed his browser's security settings to let it take actions that were commensurate with that trust. Now suppose Jane identified a cross-site scripting vulnerability in Web Site A. If she could exploit it, the result would be that her script would appear to come from Web Site A, and would therefore run using the relaxed security settings John had set for it.
- * Reading and writing cookies. Because the script would run as though it came from Web Site A, any cookies that Web Site A had set on John's computer could be accessed and modified by Jane's script.

What does this have to do with ISA Server?

When ISA Server is asked to retrieve a web page but cannot – because the page does not exist, because the server is not available, etc – it generates error information to be displayed in the user's browser. This error information takes the form of a web page, and includes the URL that was requested. However, ISA does not check the URL for the presence of script commands when generating the page, with the result that it is vulnerable to cross-site scripting.

What would this allow an attacker to do?

Like all cross-site scripting vulnerabilities, this would could potentially enable an attacker to run code in another web site's security domain, or access the site's cookies.

How might an attacker exploit the vulnerability?

The attacker could try to exploit the vulnerability in either of two ways:

- * By including a link on her web site to an unavailable page on a web site that she believed another user, operating behind an ISA Server, trusted. If she could persuade the user to visit her web site, she could cause the bogus link to fire, thereby exploiting the vulnerability.
- * By including a link within an HTML mail and mailing it to her target. The bogus link would fire when the recipient opened the mail.

How dangerous is this vulnerability?

Microsoft recommends taking all security vulnerabilities seriously. Still,

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

it can be seen that exploiting this vulnerability would be difficult, whether exploited for running script with a trusted site's security settings, or to obtain another site's cookies.

* The problem for an attacker who wanted to run code with another site's settings is that it would be difficult or impossible to know which sites another user trusts. In fact, most users do not modify their security settings from the default, in which case the attacker's code would run with exactly the same security restrictions no matter what site it appeared to come from.

* The difficult with regard to cookies is that if a web site correctly handles cookies, there wouldn't be any sensitive information in them to compromise.

I heard that some web sites keep information in cookies that couldn't be used to log on as me, but which would let someone "hijack" a session once I started it. What if the attacker used this vulnerability to read such a cookie?

It is true that some web sites keep session information in cookies, to identify the user while a session is underway. If an attacker managed to gain access to such a cookie, it could be possible to "hijack" a session, by which we mean that the attacker might be able to insert commands into the session.

However, it is important to keep this scenario in perspective.

In most cases, the attacker would have no way to know whether a particular user subscribed to a service that used such cookies.

* Even if the attacker knew that a user subscribed to such a service, there would in general be no way for the attacker to solve the timing problem – namely, how to get the user to fall victim to the attack after starting a session with the specific service the attacker wanted to hijack.

* Even if the attacker gained the session information, actually hijacking a session could be quite difficult. It would likely require the attacker to send packets "in the blind", with no way to tell whether the attack had succeeded.

What does the patch do?

The patch causes ISA Server to no longer support URL tokens within ISA Web Proxy error pages.

ADDITIONAL INFORMATION

The information has been provided by <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

Securiteam: [NT] Cross Site Scripting and Memory Leak Vulnerabi

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.

- *Previous message:* support@securiteam.com: "[REVS] Phrack 57 Is Out"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)