

# [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0060.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/16/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 16 Jun 2002 19:16:16 +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.

-----

Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

---

## SUMMARY

This patch eliminates a newly discovered vulnerability affecting Internet Information Services. Although Microsoft typically delivers cumulative patches for IIS, in this case we have delivered a patch that eliminates only this new vulnerability, while completing a cumulative patch. When the cumulative patch is customer-ready, we will update this bulletin with information on its availability. The FAQ provides information on the circumstances surrounding the vulnerability, and why we believe releasing a singleton patch immediately is in customers' best interests. To ensure that servers are fully protected against past as well as current vulnerabilities, we strongly recommend installing the previous cumulative patch (discussed in Microsoft Security Bulletin MS02-018) before installing this patch.

The vulnerability is similar to the first vulnerability discussed in Microsoft Security Bulletin MS02-018. Like that vulnerability, this one involves a buffer overrun in the Chunked Encoding data transfer mechanism in IIS 4.0 and 5.0, and could likewise be used to overrun heap memory on the system, with the result of either causing the IIS service to fail or allowing code to be run on the server. The chief difference between the vulnerabilities is that the newly discovered one lies in the ISAPI

## Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

extension that implements HTR – an older, largely obsolete scripting technology – where the previous one lay in the ISAPI extension that implements ASP.

### DETAILS

#### Affected Software:

- \* Microsoft Internet Information Server 4.0
- \* Microsoft Internet Information Services 5.0

#### Mitigating factors:

- \* Microsoft has long recommended disabling HTR functionality unless there is a business–critical reason for retaining it. Systems on which HTR is disabled would not be at risk from this vulnerability.
- \* The IIS Lockdown Tool disables HTR by default in all server configurations.
- \* The current version of the URLScan tool provides a means of blocking chunked encoding transfer requests by default.
- \* On default installations of IIS 5.0, exploiting the vulnerability to run code would grant the attacker the privileges of the IWAM\_computername account, which has only the privileges commensurate with those of an interactively logged–on unprivileged user.

#### Patch availability:

Download locations for this patch

- \* Microsoft IIS 4.0:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39579>

- \* Microsoft IIS 5.0:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39217>

Is this a cumulative patch?

No. This patch eliminates a newly discovered security vulnerability, but it is not cumulative. A cumulative patch for this issue and others is under development, and will be completed shortly. When it is available, we will update this bulletin to provide information on how to obtain it.

Because this patch is not cumulative, we recommend that customers ensure that they have installed the most recent cumulative patch (delivered in Microsoft Security Bulletin MS02–018) before installing this patch.

I thought Microsoft's policy was to provide cumulative patches for IIS.

Why isn't this patch cumulative?

Microsoft's normal policy is to provide security fixes for IIS via cumulative patches. In fact, a cumulative patch has been underway for several weeks. However, cumulative patches require extensive testing because of their scope and wide deployment. As a result, the cumulative patch is several weeks away from being customer–ready.

## Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

The newly discovered vulnerability is similar to another vulnerability (discussed in Microsoft Security Bulletin MS02-018), for which exploit tools are already available. At the same time, eliminating the vulnerability required only a small amount of code change, in a component with few dependencies on other code. As a result, we concluded that there was high value in developing a singleton patches and that we could do so in a much shorter timeframe than usual.

If I don't want to install the patch, is there a workaround procedure for this vulnerability?

Yes. As discussed below, the vulnerability can be eliminated by disabling a rarely used feature in IIS. Customers who have already disabled this feature don't need to take any additional action.

What's the scope of the vulnerability?

This is a buffer overrun vulnerability affecting IIS 4.0 and 5.0. By sending a specially chosen request to an affected web server, an attacker could either disrupt web services or gain the ability to run a program on the server. Such a program would run with full system privileges in IIS 4.0, and with fewer but nevertheless significant privileges in IIS 5.0

Microsoft has long recommended that customers remove the functionality that contains the vulnerability unless there is a business-critical reason for retaining it, and customers who have done so would be at no risk from this vulnerability. The IIS Lockdown Tool disables this functionality by default. Customers who have retained the functionality but deployed the URLScan tool as discussed in Microsoft Security Bulletin MS02-018 would likewise be protected against the vulnerability.

What causes the vulnerability?

The vulnerability results because of an arithmetic error in the ISAPI extension that implements the HTR functionality. Specifically, the error lies in a function that enables data to be uploaded to a web server via chunked encoding, and causes IIS to allocate a buffer of the wrong size to hold incoming data, with the result that the data could overrun the end of the buffer.

What is an ISAPI extension?

ISAPI (Internet Services Application Programming Interface) is a technology that enables web developers to extend the functionality of their web servers by writing custom code that provides new services for a web server. Such code can be implemented in either of two forms:

- \* As an ISAPI filter — a dynamic link library (.dll) that uses ISAPI to respond to events that occur on the server.
- \* As an ISAPI extension — a dynamic link library that uses ISAPI to provide a set of web functions above and beyond those natively provided by IIS.

In the case of this vulnerability, the affected code is an ISAPI extension that implements scripting via HTR.

## Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

What is HTR?

HTR is a first-generation advanced scripting technology delivered as part of IIS 2.0. HTR was never widely adopted, largely because a far superior technology, Active Server Pages (.ASP), was introduced in IIS 4.0 and became popular before customers had invested significant development resources in HTR. However, all versions of IIS through version 5.1 do provide support for HTR, for purposes of backward compatibility.

Microsoft has long advocated that customers disable HTR on their web servers, unless there is a business-critical need for the technology. By default, the IIS Lockdown Tool disables HTR support, by unmapping the HTR ISAPI extension.

Are there any widespread uses for HTR?

Virtually the only purpose for which HTR technology is still used today is web-based password management services. IIS ships with a set of HTR scripts that, if deployed, make it possible for users to change their Windows NT passwords via a web server, and make it possible for administrators to perform password management through the web.

In general, Microsoft recommends against performing password management over the web. However, for customers who must do this, we recommend converting any needed HTR scripts to ASP.

What is chunked encoding?

Web servers frequently need the ability to accept data from a user. For instance, when a visitor to a web site fills in a form and submits it, the data needs to be uploaded to the server so it can be processed. In cases like this, the amount of data that will be transferred is known in advance, and the server can allocate a buffer of the right size. However, in other scenarios, it's impossible to know beforehand how much data will need to be transferred. For instance, an application might be generating data as it runs, and there might be no way to know exactly how much data it will produce.

The HTTP protocol specification provides a way to handle data like this, through a process called chunked encoding. In chunked encoding, the client generates a variable-sized quantity of data called a chunk; it then tells the web server how big the chunk is and sends it. The server allocates a buffer to accommodate the incoming chunk, then receives and processes it. As the client generates additional data, it continues agglomerating it into chunks and delivering them to the server.

What's wrong with the way the HTR ISAPI extension in IIS 4.0 and 5.0 performs chunked encoding transfers?

There's an arithmetic error in the IIS 4.0 and 5.0 HTR implementations that causes them to miscalculate the size of the buffer that's needed for an incoming chunk and allocate one that's too small. The result is that the data in the chunk can overlap the end of the buffer and overwrite other data in system memory, potentially allowing the operation of IIS to be modified.

## Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

How much data could be overwritten?

By design, the client can specify a chunk of any size – if the server can't accommodate a chunk that large, it should send an error message to the client. However, in addition to causing the wrong-sized buffer to be allocated, the arithmetic error also prevents IIS 4.0 and 5.0 from placing any real limits on the size of a chunk. As a result, it would be possible for a client to send a chunk that would overwrite most or all of the memory in the IIS process

This is a critical point, because it goes to the heart of why this vulnerability poses a threat to servers. This vulnerability is an example of so-called heap overrun; because of the dynamic nature of system memory, these can be more difficult to exploit than stack overruns and may require more sophisticated skills. Data on the server can change locations from one moment to the next, impeding the attacker's ability to overwrite selected programs or data. However, in this case, the attacker wouldn't need to know where programs were located, but could instead simply overwrite large portions of system memory indiscriminately.

What would this enable an attacker to do?

An attacker who exploited this vulnerability could use it for either of two purposes.

- \* Service disruption. By overrunning the buffer with random data, the attacker could corrupt program code and cause the IIS service to fail, thereby preventing the server from providing useful service.

- \* Change the operation of the server. By overrunning the buffer with carefully selected data, the attack could overwrite program code on the server with new program code, in essence modifying the functionality of the server software.

Who could exploit the vulnerability?

Any user who was able to establish a web session with an affected server could exploit the vulnerability.

If the vulnerability were exploited to cause the IIS service to fail, what would be needed to restore normal operation?

On IIS 4.0, the administrator would need to restart the IIS service. On IIS 5.0, the service would automatically restart itself.

Why could the vulnerability only be used to cause the IIS service to fail?

If the attacker were able to overwrite system memory indiscriminately, why not overwrite all memory on the server and cause the entire operating system to fail?

Windows NT 4.0, Windows 2000 and Windows XP operate in protected mode. In protected mode, processes can only write to sections of memory they own.

As a result, it would not be possible for the attacker to overwrite the memory belonging to the operating system.

If the vulnerability were exploited to change the operation of the server software, what would the attacker be able to do?

In a nutshell, the attacker's code would gain the privileges of the

## Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

software that called it – the HTR ISAPI extension. The privileges that the attacker could gain would depend on the version of IIS in use on the server:

\* On IIS 4.0, the HTR ISAPI extension runs by default in-process – that is, as part of the IIS Service, which runs as part of the operating system itself. As a result, exploiting the vulnerability on a default IIS 4.0 installation would give the attacker complete control over the server.

\* On IIS 5.0, the HTR ISAPI extension runs by default out-of-process – that is, in the security context of a special user account called the Web Application Manager. (Web administrators may know this account better as IWAM\_computername, where computername is the name of the server). This account has significantly fewer privileges than the IIS service.

What privileges does the Web Application Manager have?

Essentially, the account has the same privileges as those of an unprivileged user who was able to log onto the server interactively. It would not enable an attacker to take administrative action, reconfigure the server, or access important files such as the Security Account Manager database.

Nevertheless, it is important not to underestimate the damage that could be caused using even these privileges. Even these privileges could be used to cause significant damage. Worse, the vulnerability could potentially give an attacker a beachhead from which to conduct additional attacks and try to obtain additional privileges.

I'm running IIS 4.0. Can I configure the HTR ISAPI extension to run out-of-process?

You can. However, a better solution is to disable it altogether.

I used the IIS Lockdown Tool to secure my server. Does it disable the HTR ISAPI extension?

Yes. All versions of the IIS Lockdown Tool remove the HTR functionality by default, in all server configurations.

I've deployed the URLScan Tool on my server. Will it protect my system against this vulnerability?

All versions of URLScan beginning with version 2.5 provide the ability to block chunked encoding requests. There are two variants of URLScan, known as "Baseline URLScan" and "URLScan-SRP". The latter variant blocks chunked encoding by default. The former can be configured to block chunked encoding, by adding an entry to the [DenyHeaders] section of URLScan.ini that reads "Transfer-Encoding:". (Note: the quotes should not be included in the entry, but there is a colon at the end of the word "Encoding").

I've disabled the HTR functionality on my IIS server. Do I need the patch?

If you've disabled the HTR functionality, you're at no risk from this vulnerability.

Securiteam: [NT] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

How does the patch eliminate this vulnerability?

The patch eliminates the arithmetic error that causes the vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[secnotif@MICROSOFT.COM](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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NT] Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)