

[NT] ISA Server – Error Page Cross–Site Scripting (Additional Details)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0070.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/17/03

To: list@securiteam.com

Date: 17 Jul 2003 20:05:07 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

ISA Server – Error Page Cross–Site Scripting (Additional Details)

SUMMARY

As we reported in our previous article:

<<http://www.secureteam.com/windowsntfocus/5RP0B20AKK.html>> Flaw in ISA Server Error Pages Could Allow Cross–Site Scripting Attack, a flaw in ISA Server allows attackers to cause the server to return an attacker's HTML/JavaScript in its response (causing the user to think the ISA server has sent it).

DETAILS

This is very similar to the problem resolved by the MS02-18 advisory. A default error page can be used to conduct cross–site scripting attacks against a legitimate user. While XSS attacks usually involve cookie theft, they can also be used to inject 'fake' login screens that appear to be hosted on a legitimate site. These login screens can then capture credentials returning them to a collector script.

Securiteam: [NT] ISA Server – Error Page Cross–Site Scripting (Additional Details)

The particular request required and the results may depend on the configuration of the server. Since many of the error pages are vulnerable to this attack, different malformed requests are likely to return exploitable results.

When attempting to access a non–existent web page protected by ISA server without the proper credentials, the browser is returned a 403 error page with the following abbreviated information.

Please try the following

- Click the refresh button
- Open the <site> home page, and then look for links

403 Forbidden – The server denies the specified URL

The URL of <site> is outputted to the browser without filtering of the username:password information allowing an attacker to inject scripting to be executed in the domain of the ISA server.

Exploit:

This test returned a page that included an iframe, when sent against our test server.

```
*http://[iframe]:test@[site]/test
```

Where [and] are replace with angle brackets and [site] is the server.

The exploit example from Thor Larholm for the MS02–18 advisory can also be applied against a vulnerable ISA installation. This leads to the use of a scripting file hosted off–site, allowing for large portions of scripting to be included in the attack.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:brett.moore@security–assessment.com> Brett Moore.

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.