

ISA Server – Error Page Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0046.html>

From: Brett Moore (*brett.moore_at_SECURITY-ASSESSMENT.COM*)

Date: 07/16/03

Date: Wed, 16 Jul 2003 11:07:24 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

=====
= ISA Server – Error Page Cross Site Scripting
=
= brett.moore@security-assessment.com
= <http://www.security-assessment.com>
=
= MS Bulletin posted: July 16, 2003
= <http://www.microsoft.com/technet/security/bulletin/MS03-028.asp>
=
= Affected Software:
= Microsoft Internet Security and Acceleration (ISA) Server 2000
=
= Public disclosure on July 16, 2003
=====

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.

== MS03-028 states ==

ISA Server contains a number of HTML-based error pages that allow the server to respond to a client requesting a Web resource with a customized error. A cross-site scripting vulnerability exists in many of these error pages that are returned by ISA Server under specific error conditions.

== MS03-028 ==

== Description ==

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

NT-Bugtraq: ISA Server – Error Page Cross Site Scripting

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.

== Exploitation ==

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.

== Solutions ==

- Install the vendor supplied patch.

== Credit ==

Based on work by Thor Larholm at Pivx.com.

<http://www.pivx.com/larholm/adv/TL001/default.htm>

Discovered and advised to Microsoft May 21, 2003 by Brett Moore of Security-Assessment.com

%-)

== About Security-Assessment.com ==

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a

