

# Cross-Site Scripting in Unparsable XML Files (GM#013-IE)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-06/0034.html>

---

**From:** GreyMagic Software (*security\_at\_GREYMAGIC.COM*)

**Date:** 06/17/03

Date: Tue, 17 Jun 2003 10:09:52 "GMT"

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

GreyMagic Security Advisory GM#013-IE

=====

By GreyMagic Software, Israel.

17 Jun 2003.

Available in HTML format at <http://security.greymagic.com/adv/gm013-ie/>.

Topic: Cross-Site Scripting in Unparsable XML Files.

Discovery date: 18 Feb 2003.

Affected applications:

=====

Microsoft Internet Explorer 5.5 and 6.0.

Note that any other application that uses Internet Explorer's engine (WebBrowser control) is affected as well (AOL Browser, MSN Explorer, etc.).

Introduction:

=====

Internet Explorer automatically attempts to parse any XML file requested individually by the browser. When the parsing process is successful, a dynamic tree of the various XML elements is presented. However, when a parsing error occurs Internet Explorer displays the parse error along with the URL of the requested XML file.

Discussion:

=====

We have found that in some cases the displayed URL is not filtered appropriately, and may cause HTML that was passed in the querystring of the URL to be rendered by the browser. This creates a classic cross-site

## NT-Bugtraq: Cross-Site Scripting in Unparsable XML Files (GM#013-IE)

scripting attack in almost any XML file that MSXML fails to read. Practically, this means that leaving XML files on your server that can't be parsed correctly by Internet Explorer and MSXML is exposing the site to a global Cross-Site Scripting attack.

We have been able to reproduce this problem in various setups, but we couldn't pinpoint the vulnerable component reliably enough. It is most likely an MSXML issue, and not a flaw in Internet Explorer itself.

Exploit:

=====

This sample shows the basic URL for injecting content:

[http://host.with.unparsable.xml.file/flaw.xml?>alert\(document.cookie\)</script>](http://host.with.unparsable.xml.file/flaw.xml?>alert(document.cookie)</script>)

Demonstration:

=====

We put together a simple proof of concept demonstration, which can be found at <http://security.greymagic.com/adv/gm013-ie/>.

Solution:

=====

Microsoft was notified on 20-Feb-2003. They reported that they were able to reproduce this flaw on IE6 Gold, and no other version. Our research showed different, yet inconsistent results (see "Tested on" section for details).

Tested on:

=====

IE5.5 NT4.

IE6 Win98.

IE6 Win2000.

Disclaimer:

=====

The information in this advisory and any of its demonstrations is provided "as is" without warranty of any kind.

GreyMagic Software is not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

Feedback:

=====

Please mail any questions or comments to [security@greymagic.com](mailto:security@greymagic.com).

