

# wp-02-0007: Microsoft SQLXML ISAPI Overflow and Cross Site Scripting

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-06/0111.html>

---

**From:** Matt Moore ([matt@westpoint.ltd.uk](mailto:matt@westpoint.ltd.uk))

**Date:** 06/13/02

Date: Thu, 13 Jun 2002 11:10:48 +0100  
From: Matt Moore <[matt@westpoint.ltd.uk](mailto:matt@westpoint.ltd.uk)>  
To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Westpoint Security Advisory

Title: Microsoft SQLXML ISAPI Overflow and Cross Site Scripting

Risk Rating: Medium

Software: Microsoft SQLXML 3.0 / IIS 5.0 / SQLServer 2000

Platforms: Win2K

Vendor URL: [www.microsoft.com](http://www.microsoft.com)

Author: Matt Moore <[matt@westpoint.ltd.uk](mailto:matt@westpoint.ltd.uk)>

Date: 12 June 2002

Advisory ID#: wp-02-0007.txt

CVE#: CVE-CAN-2002-0186 (XSS) and CVE-CAN-2002-0187 (Overflow)

Overview:

=====

SQLXML allows XML data to be transferred to and from SQL Server, returning database queries as XML.

SQLXML has two vulnerabilities: a buffer overflow in the SQLXML ISAPI filter, and a cross site scripting vulnerability.

More complete details on how SQLXML works can be found in Microsoft's advisory (see below).

Details:

=====

Cross Site Scripting

-----

Part of the functionality of SQLXML is being able to run SQL queries via a URL such as:

```
IIS-server/Northwind?sql=SELECT+contactname,+phone+FROM+Customers+FOR+XML
```

This will return an XML document containing the query results.

## SecurityFocus Bugtraq: wp-02-0007: Microsoft SQLXML ISAPI Overflow and Cross Site Scripting

It is possible to specify an extra parameter in the query, 'root', which returns the data as above, but with a 'root' tag of the xml document as the user specified.

This feature can be used to perform cross site scripting attacks against the web application running on the server:

```
IIS-server/Northwind?sql=SELECT+contactname,+phone+FROM+Customers+FOR+XML&ro
```

```
ot=<SCRIPT>alert(document.domain)</SCRIPT>
```

Best practice recommends against allowing ad hoc URL queries against a database.

### SQLXML ISAPI Filter Buffer Overflow

---

When making SQL queries using the 'sql=' functionality of SQLXML it is possible to specify certain parameters which affect the returned XML (e.g. xsl=). One of these parameters lets you set a content-type.

It's possible to crash IIS by requesting an overly long string in the ?contenttype= parameter. This could also allow arbitrary code to be run on the server in the context of the SYSTEM account.

A normal request looks like (in this case, a direct sql= query):

```
IIS-server/demos?sql=select+*+from+Customers+as+Customer+FOR+XML+auto&root=r
```

```
oot&xsl=custtable.xsl&contenttype=text/html
```

By specifying >240 characters for the content-type parameter it is possible to make inetinfo.exe crash.

E.g. (using a 'template' file rather than a direct query, in this case):

```
IIS-Server/Nwind/Template/catalog.xml?contenttype=text/AAAA...AAA
```

### Patch Information:

---

Microsoft has released patches and an advisory for the identified issues.

These are available from:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/>

[bulletin/MS02-030.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-030.asp)

This advisory is available online at:

<http://www.westpoint.ltd.uk/advisories/wp-02-0007.txt>

---

SecurityFocus Bugtraq: wp-02-0007: Microsoft SQLXML ISAPI Overflow and Cross Site Scripting

- **Previous message:** [snsadv@lac.co.jp](mailto:snsadv@lac.co.jp): "[SNS Advisory No.54] Active! mail Executing the Script upon the Opening of a Mail Message Vulnerability"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)