

# [NT] Additional Information on MSSQLXML ISAPI Overflow and Cross-Site Scripting

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0117.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/24/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Mon, 24 Jun 2002 22:09:46 +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.

-----

Additional Information on MSSQLXML ISAPI Overflow and Cross-Site Scripting

---

## SUMMARY

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 our previous article: <http://www.securiteam.com/windowsntfocus/5LP0B0U7FC.html>

Unchecked Buffer in SQLXML Could Lead to Code Execution.

## DETAILS

Vulnerable systems:

- \* Microsoft SQLXML 3.0

Cross Site Scripting

Part of the functionality of SQLXML is available via a URL similar to:

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

This will return an XML document containing the query results.

## Securiteam: [NT] Additional Information on MSSQLXML 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
&root=<SCR!PT>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 that affect the returned XML (e.g. xsl=). One of these parameters lets you set a content-type.

It is 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=root&xsl=custtable.xsl&contenttype=text/html
```

By specifying more than 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>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[matt@westpoint.ltd.uk](mailto:matt@westpoint.ltd.uk)> Matt 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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[UNIX] Simpleinit File Descriptor Security Vulnerability"
  - ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)