

# [NT] Combing IE and .XLA leads to Security Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0141.html>

---

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

*Date:* 07/31/02

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

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

Date: Wed, 31 Jul 2002 19:43:31 +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.

-----

Combing IE and .XLA leads to Security Vulnerabilities

---

## SUMMARY

If an Internet Explorer user visits specially designed web page, the page may create almost completely arbitrary files on the user's computer. This could in turn lead to executing arbitrary programs on the user's computer.

## DETAILS

Vulnerable systems:

\* Office XP and Internet Explorer version 6.0

This is not a completely new issue, but the involvement of IE makes it worth noting. [1] (from March 2002) Describes a problems with Microsoft's spreadsheet component [2] and in its Host() function which may be exploited to create a file.

Microsoft tried to produce a partial patch to the issue, but the problem was not completely solved. It is possible to create a .XLS or .XLA file, which in turn is able to write files with the help of OWC. The .XLA file is just an .HTML file with an .XLA extension.

Another interesting problem is [3] from 2000. The key point in it is that IE can be caused to invoke Excel with `<object data="file.xls"></object>`.

## Securiteam: [NT] Combing IE and .XLA leads to Security Vulnerabilities

Though not visible, Excel executes "file.xla", which may contain tricks from [1], causing the OWC to run the SaveAs() function, causing the creation of arbitrary files.

Workaround/Solution:

1) Under IE disable "Run ActiveX controls and plugins".

Alternatively:

2) Deregister and delete the ms office spreadsheet component and/or all the OWC. This may be done by going through the following procedure:

Control Panel – Add/Remove programs – Office – Change (then look for OWC)

→ Remove the OWC package

Vendor status:

Microsoft was notified several days ago – they have opened a case on this report.

### ADDITIONAL INFORMATION

References:

[1] Georgi Guninski security advisory #53, 2002 – More Office XP problems – Version 3.0 – 31 March 2002

<<http://www.securiteam.com/windowsntfocus/5OP010A6UO.html>> New Office XP Security Problems Discovered.

[2] The spreadsheet component from OWC is well documented on the office CDs.

[3] Georgi Guninski security advisory #13, 2000 – IE 5 and Excel 2000, PowerPoint 2000 vulnerability – executing programs

<<http://www.securiteam.com/windowsntfocus/5PR090A1O1.html>> IE 5 with Office 2000 vulnerable to remote command execution.

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](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.

Securiteam: [NT] Combing IE and .XLA leads to Security Vulnerabilities

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Protected Adobe eBooks can be copied between Computers"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)