

[NT] Combining IE and .XLA leads to Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0144.html>

From: support@securiteam.com

Date: 07/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 31 Jul 2002 20:02:57 +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.

Combining 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] Combining 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 proce