

[NT] Internet Explorer Popup OBJECT Tag Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0067.html>

From: support@securiteam.com

Date: 01/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 15 Jan 2002 09:22:43 +0100 (CET)

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.

Internet Explorer Popup OBJECT Tag Bug

SUMMARY

The Popup object allows the insertion of embedded objects. Those objects run in a high privilege space allowing the execution of local applications by a remote attacker.

DETAILS

Vulnerable systems:

Internet Explorer 6.0.2600.0000

Exploits:

An exploit code is available at:

<<http://www.osioniusx.com>> <http://www.osioniusx.com>

"funRun.html" -- This page shows how you can run just about anything you want on a Windows system remotely from IE if it is on the user's system.

It includes two sections: one section demonstrating running applications through the popup object; the second section demonstrating opening up control panels and the like from the earlier released bug

"directoryInfo.html", i.e. the "<file:///:::{CLSID}>" feature of IE.

Workaround:

Disable ActiveScripting.

Securiteam: [NT] Internet Explorer Popup OBJECT Tag Bug

ADDITIONAL INFORMATION

The information has been provided by <mailto:osioniusx@yahoo.com> the Pull.

=====

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: "[NEWS] Shockwave Flash Player Security Issue"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)