

[NT] JavaScript in IE Can Take Over the Whole Screen

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0054.html>

From: support@securiteam.com

Date: 10/22/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] JavaScript in IE Can Take Over the Whole Screen

Message-Id: <20011021222536.E0E3D138C9@mail.der-keiler.de>

Date: Mon, 22 Oct 2001 00:25:36 +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.

JavaScript in IE Can Take Over the Whole Screen

SUMMARY

The following is not security vulnerability by itself but has some security implications. It is possible for a web page containing JavaScript to take over the whole screen – including menus, modal dialogs, taskbar, clock, etc. This allows for malicious web sites to "spoo" the whole screen including modal IE messages. This means that a script initiated IE dialog "You are downloading malicious.exe from malicious.com – 'Open | Cancel |more info'" may be made to appear to the user:

"Welcome to my new site – 'Open'" ('Cancel' is not visible and not clickable) If the user clicks on 'Open' in the spoofed context code may be executed (user interaction is required).

DETAILS

Vulnerable systems:

Internet Explorer version 5.5/6.0 on Windows, probably earlier versions

Spoofing the UI is done by `window.createPopup()` and `popup.show()` –

Securiteam: [NT] JavaScript in IE Can Take Over the Whole Screen

```
op=window.createPopup();
op.document.body.innerHTML="...html...";
op.show(0,0,screen.width,screen.height,document.body);
-----
```

Demonstration:

Image moving over download/open dialog:

<<http://www.guninski.com/opf2.html>> <http://www.guninski.com/opf2.html>

BSOD emulation:

<<http://www.guninski.com/bsod1.html>> <http://www.guninski.com/bsod1.html>

Workaround:

If you consider this to be a threat, disable "active scripting"

Vendor status:

Microsoft was informed on 16 October 2001.

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: "[TOOL] UNIX System Call Tracker"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)