

# [NT] IE Chromeless Window Vulnerabilities (More Examples)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0056.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 07/15/03

To: list@securiteam.com

Date: 15 Jul 2003 19:05:27 +0200

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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
IE Chromeless Window Vulnerabilities (More Examples)  
-----

## SUMMARY

A window without a frame, title bar, toolbars or scroll bars is known as a 'chromeless' window. If a chromeless window can be opened on top of other windows, it is possible to impersonate Windows user interface elements.

Why is this a security problem? Because Windows and browser UI elements are themselves, part of security mechanisms. If the UI for security features can be faked, users can be tricked into making inappropriate decisions.

The 'traditional' way of doing chromeless windows was to use the DHTML method `window.open` to open a full-screen browser window (which is chromeless) and then resize this to smaller dimensions. This capability was removed in IE6 Service Pack 1, presumably due to exactly these security concerns.

## DETAILS

## Securiteam: [NT] IE Chromeless Window Vulnerabilities (More Examples)

It is still possible to get chromeless windows by using the `window.createPopup` method. A window opened with `createPopup` has some unusual properties:

- It is closed when one clicks on the outside the popup. This is easy to circumvent by simply re-spawning it on close.
- It cannot be focused. (It is impossible to put controls like text input fields in it; this, at least, prevents us from overlaying fake login forms onto other websites.) Focus stays with the opener window.
- It floats above other normal windows, allowing it to obscure them even whilst they are focused.

One popup may be created per window, allowing one to overlay an arbitrary rectangle of screen display area with fake UI. Overlays that are more complicated can be achieved by having multiple windows opening popups at once; a popup is itself a window so can be used to open further popups.

Examples:

All browser-based SSL security cannot be trusted:

The attacker can direct you to an unencrypted site under his control and cover up his site's malicious address in the address bar with "<https://www.etrade.com/>" (or whatever) to make the user think he/she's really at your web site; someone malicious can even cover up the broken padlock with a gold padlock in the status bar, cover up the certificate warning, etc. And, even if you type in the URL yourself to be sure you're going to the right site, there's no way to know whether your address bar isn't actually a text box on a malicious form from some other page that's covering up your real address bar and redirecting you to the attacker's site.

Any Windows application username & password can be intercepted:

The user's desktop can be replaced with a full-screen fake desktop (Start button and all) that has a malicious password dialog in it that looks just like the real thing (or just the malicious dialog all on its own outside of the border of IE). Think of the usernames and passwords a malicious person could get by displaying a Windows/Novell/Outlook/PeopleSoft/etc. Password dialog in the middle of an employee's screen (you could even add a depressed button in their taskbar to look like the window was open, make the window draggable by the title bar, etc.). When the victim enters their authentication credentials and clicks OK, their credentials are submitted via a form to a malicious web site.

ActiveX signing dialogs cannot be trusted:

They can be obscured to look like any application dialog in the world that you would click Yes on, and the No and Cancel buttons can be hidden. Or, someone malicious can just cover up "This control is unsafe/unsigned" with "This control has been signed by Microsoft, Inc.", complete with hyperlinkable text that works like the real thing.

## Securiteam: [NT] IE Chromeless Window Vulnerabilities (More Examples)

Although the example given by Andrew is currently slow, this page should scare you (move the ActiveX dialog around after it has fully loaded):

<<http://www.doxdesk.com/personal/posts/bugtraq/20030713-ie/activex.html>>  
<http://www.doxdesk.com/personal/posts/bugtraq/20030713-ie/activex.html>

All of this is possible because the user clicked on a link or opened a page — they did not have to click Yes on any JavaScript popup or ActiveX dialog, and these are just the obvious problems.

Solution:

window.createPopup() should have the same chromeless window restrictions as createModalDialog() and createModelessDialog().

Vendor response:

Microsoft was informed of the problem on 23 January. After initially encouraging e-mails, no action has been taken since.

Andrew is posting this issue now as Andrew has seen it being exploited in the wild.

If you use IE, be extremely wary of trusting what appear to be its built-in security controls.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:and-bugtraq@doxdesk.com> Andrew Clover and <mailto:ops-lists@positivenetworks.net> Jason Sloderbeck.

=====

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.