

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00040.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 13 Feb 2006 13:38:58 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Microsoft Internet Explorer Drag-and-Drop Redeux

SUMMARY

Microsoft Internet Explorer suffers from a vulnerability in its handling of certain drag-and-drop events. As a result, it is possible for a malicious web site to predict and exploit the timing of a drag-and-drop operation such that any drag operation (including using scroll-bars) could potentially lead to the installation of arbitrary files in sensitive locations that may enable further system compromise.

DETAILS

Affected Systems:

- * Microsoft Internet Explorer 5.01
- * Microsoft Internet Explorer 5.5
- * Microsoft Internet Explorer 6.0
 - Windows 98
 - Windows 98 Second Edition
 - Windows Millennium Edition
 - Windows 2000
 - Windows XP
 - Windows Server 2003

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

As a result of recent updates to its drag-and-drop functionality, Internet Explorer now imposes a rigid set of restrictions on most drag-and-drop sources:

- * Input to the browser from other applications is not permitted.
- * Dragging an object from inside a frame is not permitted.
- * Dragging an HTML element from a top-level window will produce a security warning.

However, certain objects not derived from an HTML document (specifically, file objects within a folder view) remain draggable. This gives rise to a potential race condition in the handling of user input. If an attacker can persuade a user to drag any object within the top-level window that his/her site is contained in, malicious script can redirect these inputs to other top-level windows, potentially resulting in an unintended consequence such as file installation.

Proof-of-concept code has been developed that utilizes a pop-under window pointing to a malicious file share. This window can be created using `window.open()` or other stealthier methods that are known to evade Internet Explorer's built-in pop-up blocking. Focus is then returned to the opening window, where the user is encouraged to drag an object (image, link, etc.) in a seemingly "safe" fashion.

Immediately prior to this object being dragged, a `mouseover` event is triggered that enables the attacker to (with a varying degree of success) predict the imminent drag attempt. The pop-under can then be returned to focus by way of a `window.blur()` executed in the current window. If the timing of the transition is accurate to a margin of error within a user's reaction time threshold, the user will unwittingly initiate a drag of a file from the pop-under instead of the object originally used as a lure by the attacker.

As soon as it transfers focus, the window with the original interactive content may set a timer (via `window.setTimeout()`) that returns focus to the window with a simple `window.focus()` call. After a split-second delay, focus is returned to the interactive window. At this point, on-demand alteration of CSS attributes can be used to display previously-hidden objects (such as inline frames). These objects serve as "drop target" windows and will initiate the copying of the file dropped from the (presumably malicious) pop-under window.

While Internet Explorer blocks hiding or resizing of certain "suspect" objects (IFRAMEs, for instance), so-called container objects (DIV, SPAN, etc.) suffer no such restrictions, even when they contain one of the objects in the former category. The proof-of-concept code as developed simply stores a full-screen inline frame in a container initially marked with the "hidden" visibility style.

The pop-under window, in this instance, would be a folder on a malicious server. This could be accessed via SMB (`\\HOSTILESERVER\SHARE`), FTP

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

(<ftp://hostileserver/somedirectory>) or even HTTP (web folders) using certain link behaviors in combination with the click() method of a hyperlink object. In the third case, the pop-under would be targeted to an HTML document initially, which would then open the web folder containing hostile content.

The path to the drop target (the hidden frame in the original window) requires a little more creativity. Particularly in Windows XP Service Pack 2, Microsoft has done a fairly good job of locking down access to local resources. The most interesting vector for the purposes of this attack is via the network redirector. By using the IP address or machine name of the local system (typically obtainable via any number of means), such as:

```
\\MACHINENAME\share
```

It becomes possible to access resources offered by the network redirector on the local system. Of most interest is the "Scheduled Tasks" folder:

```
\\MACHINENAME\Scheduled Tasks
```

Items dropped into this folder execute automatically at a system-determined time (3 AM local time in tests on Windows XP Professional Service Pack 2) each day as the user dropping the file. Also of interest are common shares such as the administrative shares (C\$, D\$, etc.) and typical share names like "SharedDocs" on Windows XP. In most cases, this is at least a partial functional equivalent to local file system access and is not subject to zone restrictions, even on Windows XP Service Pack 2.

Impact:

A malicious web site, with a minimum of social engineering, may be able to compromise user systems by triggering an unintended installation of malicious software. Typical defense-in-depth measures may mitigate this issue. For those who run Internet Explorer with administrative privileges, the impact of any successful exploitation is complete control of the affected system. A malicious web site could install software that would add or delete privileged user accounts, alter, destroy or disclose the content of personal or otherwise sensitive files, record personal information or any number of other activities.

Users who do not browse with such high levels of privilege would be at a significantly reduced risk from exploitation of this vulnerability. In the case of a user with limited privileges, this vulnerability could only be exploited by an attacker to install software that executes with the privileges of that user.

Workaround:

The following workarounds are believed at the time of this writing to be effective against the exploitation of this vulnerability in some form:

1. Set a Kill Bit on the Shell.Explorer Control

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

Setting a kill bit on this control will prevent Internet Explorer from displaying the rich folder view interface that gives rise to this attack. For more information about setting kill bits, please see Microsoft Knowledge Base Article 240797: <<http://support.microsoft.com/kb/240797>>
<http://support.microsoft.com/kb/240797>

The CLSID of this component as deployed on Windows XP is:
{8856F961-340A-11D0-A96B-00C04FD705A2}

Tools to automate the process of setting this kill bit have been provided at: <<http://student.missouristate.edu/m/matthew007/tools/shellkill.zip>>
<http://student.missouristate.edu/m/matthew007/tools/shellkill.zip> PGP signature:

<<http://student.missouristate.edu/m/matthew007/tools/shellkill.zip.asc>>
<http://student.missouristate.edu/m/matthew007/tools/shellkill.zip.asc>

Included in this archive are an Administrative Template (.adm) and a VBScript file (.vbs) which implement this setting. The Administrative Template also allows an administrator to work around a specific case of functionality loss caused by the implementation of this workaround. Instructions on using both files are contained within the readme file in the archive.

IMPACT: This workaround will cause Internet Explorer to no longer render folder views for local directories, network file shares, FTP directories and web folders by default. The ability to browse FTP directories in Internet Explorer can be restored by clearing the "Enable Folder View for FTP Sites" option in Internet Explorer's "Advanced" options. However, this countermeasure is known to expose another security vulnerability that does not appear to have been fixed as of this writing:

<<http://lists.grok.org.uk/pipermail/full-disclosure/2003-June/005321.html>>
<http://lists.grok.org.uk/pipermail/full-disclosure/2003-June/005321.html>

For ordinary browsing purposes, the Windows Explorer tool is unaffected by this change. This defensive measure has been successfully implemented in at least one commercial software product and tested on a significant scale prior to the release of this advisory. Therefore, it is the belief of the author that potential loss of functionality *should* be minimal. As with all measures, you are encouraged to test the impact of this workaround prior to making any decision about deployment.

2. Prevent Automatic Navigation to Local Intranet Zone (Windows XP SP2, Windows Server 2003 SP1)

This workaround will prevent Internet content in Internet Explorer from automatically navigating to URLs within the Local Intranet Zone. This effectively prevents the introduction of malicious code to the local system via the network redirector. To implement this workaround, follow these steps:

1. In Internet Explorer's Tools menu, choose "Internet Options..."
2. Select the "Security" tab and choose "Local Intranet"

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

3. Click the "Custom Level" button
4. Set the "Web sites in less privileged content zone can navigate into this zone" setting to "Disable" or "Prompt".
5. Click OK to close any dialogs and optionally, close Internet Explorer.

IMPACT: This workaround will block or prompt before allowing any navigation to LAN resources from the Internet Zone. Direct access to LAN resources continues to function normally. As a result of this workaround, attempts to access local intranet content (for instance, web applications on corporate Intranets) from web sites outside of the LAN will fail or produce prompts, depending upon the chosen setting.

3. Disable Active Scripting

This workaround will prevent Internet content from executing script that could potentially cause the exploitation of this vulnerability. To implement this workaround, follow these steps:

1. In Internet Explorer's Tools menu, choose "Internet Options..."
2. Select the "Security" tab and choose "Internet"
3. Click the "Custom Level" button
4. Set the "Active scripting" option to "Prompt" or "Disable".

IMPACT: This workaround will block or prompt before allowing web sites to execute any script statement. Scripting in more-privileged zones (Local Intranet, Trusted Sites) continues to function normally. Setting this option to "Prompt" may cause a significant increase in the number of security prompts received while browsing and may be ineffective in closing this vulnerability for users not capable of making an assessment of a web site's relative trustworthiness.

Mitigation Recommendations:

1. Limit Viewing to Trusted Web Sites

In some situations, browsing can be successfully limited to only trustworthy sites without significant loss of productivity. Users should be extremely cautious while browsing unknown or untrusted web sites, as such web sites are often able to introduce hostile code.

2. Run Exposed Applications With Reduced Privilege

Users who log on interactively without the privileges of powerful groups such as the "Administrators" or "Power Users" groups are at a much lower risk of damage from successful exploitation of software vulnerabilities in client applications. This mitigation step greatly reduces the likelihood of a successful malware installation if this vulnerability is exploited.

Vendor response:

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

Microsoft was informed of this vulnerability on August 3, 2005. Currently, the company has no plans to issue a security update to correct this vulnerability. Fixes for this issue are scheduled to be included in Service Pack 2 of Windows Server 2003 and Service Pack 3 of Windows XP. Of particular note is that Windows 2000 users will *NOT* receive an update to correct this vulnerability.

Microsoft's internal risk-assessment concluded that this issue was not sufficiently serious to be fixed in a security bulletin. This conclusion appears fundamentally inconsistent with the way related issues were handled by Microsoft. In particular, the drag-and-drop vulnerability patched by MS05-013 received an "Important" rating.

I disagree with the technical conclusion behind Microsoft's decision and I further find the timeframe of delivery and deployment for maintenance releases to be largely unsuitable for security fixes of any significant magnitude. I find the harm this decision could potentially inflict upon down-level users (most importantly, users of Windows 2000) to be unjustified by the technical concern Microsoft has raised to me. Microsoft also rejected a request that it consider the issue for inclusion in a later security update as a "Moderate" risk issue.

Due to Microsoft's noncommittal and generally unimpressive response to the issue, this advisory is being issued to inform users of this vulnerability such that defensive action may be taken as desired.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3840>>
CVE-2005-3840

OSVDB:

The Open Source Vulnerability Database (OSVDB) project has assigned OSVDB vulnerability ID #2707 to this issue. Information will be available shortly after the publication of this advisory at the following URL:
<http://www.osvdb.org/displayvuln.php?osvdb_id=2707>
http://www.osvdb.org/displayvuln.php?osvdb_id=2707

SecurityTracker:

SecurityTracker has pre-assigned an alert number in its internal database to reference this issue. Information will be available shortly after the publication of this advisory at the following URL:
<<http://www.securitytracker.com/id?1015049>>
<http://www.securitytracker.com/id?1015049>

SecurityFocus:

SecurityFocus has pre-assigned BugTraq ID #15089 to reference this issue. Information will be available shortly after the publication of this advisory at the following URL: <<http://www.securityfocus.com/bid/15089>>
<http://www.securityfocus.com/bid/15089>

Acknowledgements:

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

[NT] Microsoft Internet Explorer Drag-and-Drop Redeux

The Administrative Template file supplied in the workaround ZIP was authored by Steven Platt.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mattmurphy@xxxxxxxx>>
Matthew Murphy.

=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.