

Aviv Raff On .NET - Internet Explorer "Print Table of Links" Cross-Zone Scripting Vulnerability

Aviv Raff On .NET - Internet Explorer "Print Table of Links" Cross-Zone Scripting Vulnerability - Aviv Raff, aviv.raffon.net.

- Published: date not stated
- Original:
<<https://web.archive.org/web/20080519094504/http://aviv.raffon.net/2008/05/14/InternetExplorerPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx>>
- Preserved from:
<https://web.archive.org/web/20080519094504/http://aviv.raffon.net/2008/05/14/InternetExplorerPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx> (live) on 2026-08-10
- Capture timestamp: 20080519094504
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Aviv Raff On .NET - Internet Explorer "Print Table of Links" Cross-Zone Scripting Vulnerability

The Wayback Machine -

<https://web.archive.org/web/20080519094504/http://aviv.raffon.net:80/2008/05/14/InternetExplorerPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx>

| | |

| | | |

|

Wednesday, 14 May 2008

| | |

| |

|

[Internet Explorer "Print Table of Links" Cross-Zone Scripting Vulnerability](#)

| | |

Summary

Internet Explorer is prone to a Cross-Zone Scripting vulnerability in its “Print Table of Links” feature. This feature allows users to add to a printed web page an appendix which contains a table of all the links in that webpage.

An attacker can easily add a specially crafted link to a webpage (e.g. at his own website, comments in blogs, social networks, Wikipedia, etc.), so whenever a user will print this webpage with this feature enabled, the attacker will be able to run arbitrary code on the user’s machine (i.e. in order to take control over the machine).

Affected version

Internet Explorer 7.0 and 8.0b on a fully patched Windows XP.

Windows Vista with UAC enabled is partially affected (Information Leakage only).

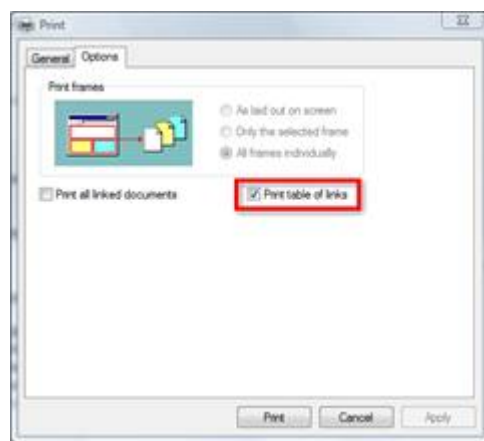
Earlier versions of Internet Explorer may also be affected.

Technical details

Whenever a user prints a page, Internet Explorer uses a local resource script which generates a new HTML to be printed. This HTML consists of the following elements: Header, webpage body, Footer, and if enabled, also the table of links in the webpage.

While the script takes only the text within the link’s inner data, it does not validate the URL of links, and add it to the HTML as it is. This allows to inject a script that will be executed when the new HTML will be generated.

As I said in a [previous post](#), most of the local resources in Internet Explorer are now running in Internet Zone. Unfortunately, the printing local resource script is running in Local Machine Zone, which means that any injected script can execute arbitrary code on the user’s machine.



Proof of Concept

The following is an example of a URL which executes Windows Calculator:

[http://www.google.com/?q=<script defer>new ActiveXObject\("Wscript.Shell"\).run\("calc"\)</script>](http://www.google.com/?q=<script defer>new ActiveXObject()

I removed the proof-of-concept of the [Oday treasure hunt](#). A live proof-of-concept can be found [at milw0rm](#).

Solution / Suggestion

I've contacted Microsoft last Tuesday. Their last response was that they are looking at an appropriate fix.

Until a patch is available, I suggest not to use the “print table of links” feature when printing a webpage.

| | |

Wednesday, 14 May 2008 13:12:52 UTC | | [Security](#)

(<https://web.archive.org/web/20080519094504/http://aviv.raffon.net/2008/05/14/InternetExplorerQuotPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx>)

| |

| | |

| |

| | | |

|

| |

Archived from <https://web.archive.org/web/20080519094504/http://aviv.raffon.net/2008/05/14/InternetExplorerQuotPrintTableOfLinksquotCrossZoneScriptingVulnerability.aspx>. Rendered offline from the local Markdown copy.