

[Full-disclosure] Pincone Research Clipboard Access

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-08/msg00677.html>

- *From:* "y0himba" <y0himba@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 25 Aug 2006 16:09:48 -0400
-

Hi there.

Sorry for the book in advance. I am not half as intelligent as some of you, and this list is extremely informative, but I don't "speak up" much. I have an issue, and maybe you guys can shed some light on it, and the risks it can pose.

I do surveys at a site "www.pineconeresearch.com". They are usually opinions on new products. It's fairly interesting to see what garbage the conglomerates are thinking up to separate us from our money, plus, I get a whole \$5 for each survey. Oh yay. I have been doing this some time now, over 2 years.

This issue affects IE only, they do not allow the use of Firefox for surveys there any more, which is BS to me in the first place.

The have implemented a "security feature" that attempts to access my clipboard. I of course don't want to allow this, so I emailed the person "in charge" explaining the problem with accessing the survey. Her recommendation was to "enable clipboard access by websites". See her email below. When calling the contact number, you instantly get shunted to the "high call volume" menu and get to leave a message. NO ONE ANSWERS, EVER.

What should I do from here? It's an extremely popular site, and the person in charge is telling folks to allow websites access to the clipboard.

Thanks for your help on this if any.

-----Original Message-----

From: <-snip->
Sent: Thursday, August 24, 2006 3:18 PM
To: <-snip->
Subject: PineCone Research

Dear Panelist,

I apologize for the difficulty. This is a security feature built into

[Full-disclosure] Pincone Research Clipboard Access

newer versions of IE. Some panelists reporting this issue have resolved it by adjusting their security settings using one of the following methods:

With Internet Explorer open, go to Tools, Internet Options and select the Security tab. Under "Select a zone to view or change security settings." click Internet. Select Custom Level. Scroll down almost to the bottom to find something labeled Scripting. Under that there is "Allow Programmatic clipboard access" where you can choose Enable.

OR, depending on your version of IE:

With Internet Explorer open, go to Tools, Internet Options and select the Security tab. Under "Select a zone to view or change security settings." click Internet. Select Custom Level. Scroll down almost to the bottom to find something labeled Scripting. Under that there is "Allow Paste Operations via script," where you can choose Enable.

Thank you for your patience!

Thank you again,

---my responses---

Karen,

One of the things that my business does it security checks. This is a very easy way to grab a user's password, they copy it to the clipboard, then hit a page that grabs that from the clipboard without their knowledge.

I cannot allow web pages access to my clipboard. The "fix" you are describing is an EXTREMELY insecure thing to do, allowing any webpage the ability to read/write to the clipboard, opening a remote code execution vulnerability, buffer over/under runs, and if there is sensitive information on the clipboard, it can be read.

This security featured is flawed, and needs to be changed. I enjoy filling out the surveys, seeing possible new products, but I cannot allow that security breach, sorry. Hopefully your IT people will change this? Surely you realize that allowing virus code or other to be written to the clipboard is dangerous? If you have copied your home phone, credit card number, or something else of that sort to the clipboard it can be read this way.

---response 2---

I have Internet Explorer 6+ and IE7 beta. Your "security" measure is a "security" risk and a privacy issue. Your fix outlined in an earlier email recommends ALLOWING WEBSITE FREE READ/WRITE ACCESS TO A USER'S CLIPBOARD, potentially allowing code to be copied to the clipboard, or allowing private, sensitive information to be collected form the clipboard by a website.

[Full-disclosure] Pincone Research Clipboard Access

I have reported this to several security and privacy websites, long with a copy of the email you sent outlining how to disable this IE security feature. It has also been posted to the Full-Disclosure mailing list.

You may want to reconsider your "fix" for your insecure, flawed "security" feature. It is easy to extrapolate that your "fix" may cause a user's private information to be copied by a 3rd party, identity theft or credit card charges to occur from that, a direct result of your "fix", which will result in a lawsuit naming your company or you specifically as the cause.

-----BEGIN GEEK CODE BLOCK-----

Version: 3.1

GCM/GIT/GO d- s: a C++++\$ UL++++ P++++ L++++ E++++ W++++ N+++++ o++++ K++ w
O- M- V-- PS+ PE Y++ PGP++ t+ 5-- X+++++ R* tv++ b+++++ DI++ D++++ G++ e
h---- r+++ y++++

-----END GEEK CODE BLOCK-----

Get Your Geek Code: <http://www.geekcode.com>

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>