

Re: Software Restriction Policy flaw

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2008-05/msg00090.html

- *From:* Kam <Kam@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 7 May 2008 10:41:01 -0700
-

Try using these policies:

1. Within IE, disable the "File > Open" menu option.
2. Enable the "Allowed Windows Apps" policy, and populate that list with applications that you wish to allow.
3. Prevent access to C: drive + disable file browsing so that they can't go searching for the app.
4. Disable the Run-As option

"Jeremy Harrington" wrote:

I didn't expect it to be new, I'm just hoping someone has come up with something half-way intelligent as a fix since 2006 (when that particular post was created).

"Shenan Stanley" wrote:

Jeremy Harrington wrote:

I have deployed a Group Policy for a certain subset of users that only allows them to use Internet Explorer. To do so, I set Software Restriction with a default setting of "Deny," with the only exception being IE. With basic testing, it seems to work perfectly.

However, if you perform the following steps from within IE, you can run any application, in complete disregard for the GP.

- 1) Open IE
- 2) Go to File->Open
- 3) Click the "Browse" button
- 4) Change the "Files of Type" drop down to "All Files"
- 5) Browse to any app that shouldn't run.
- 6) Hold down CTRL-SHIFT while right clicking the app to

Re: Software Restriction Policy flaw

bring up
the "Run As" option and click "Run As"
7) Leave the default options (current user with checked box)
selected and click "Ok"

I tried this with multiple applications, and it worked every
time.
The fact that 99% of users will never try this is irrelevant.
This
makes software restriction security by obscurity, rather than
a
tool to be counted on.

Not new. Google on it?

June 2006 article:

<http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-06/msg00243.html>

(Including a supposed response from Microsoft concerning the 'issue'...)

Shenan Stanley
MS-MVP

How To Ask Questions The Smart Way

<http://www.catb.org/~esr/faqs/smart-questions.html>