

## Re: Ten least secure programs

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-07/0371.html>

---

**From:** David (*dcorking\_at\_yahoo.fr*)

**Date:** 07/06/03

Date: Sun, 6 Jul 2003 13:39:14 -0400  
To: security-basics@securityfocus.com

On Wed, 02 Jul 2003, Chris Berry wrote:

> >From: "Roger A. Grimes" <rogerg@cox.net>  
> >By disabling "ActiveX", you'll be telling your users they can only have a  
> >limited experience (HTML, graphics, scripting) with IE. Not completely  
> >unsound, but most users will revolt.  
>  
> Then the revolution will be crushed without mercy. Just like when we  
> implemented site restrictions, although that one wasn't my idea.  
>  
> >Disable all ActiveX and then surf. You'll not be able to read most  
> >popular web sites.  
>  
> Ahhum....Bulls\*\*\*  
>

I agree with Chris. I normally surf with ActiveX set to "Prompt"

When prompted I normally refuse and rarely miss out on content.

>  
> >It won't load Flash, RealPlayer, Windows Media Player, or most other  
> >plug-ins or Helper  
> >Applications.  
>  
> Good, 95% of these have no legitimate business application anyways, and if  
> they do I can enable them for that user.

The Acrobat Reader plug-in is considered by IE to be an ActiveX control. This is where I have to say yes when prompted.

Some websites still fail to show the Acrobat Reader – which I have guessed was caused by poor javascript code. I have had similar difficulties with Netscape (and also with other types of ActiveX content – and some webmasters still post unsigned ActiveX content – "what is that all about?" – a client of mine recently bought an intranet server application whose ocx controls IE6 reports as

## SecurityFocus BASICS: Re: Ten least secure programs

unsigned – I bet that will annoy their desktop admin.)

I don't know if there is a config in IE that will allow some plug-ins and not others. At the cost of speed, though, I think Acrobat Reader can be configured as a helper app instead of a plug-in.

I have heard of the potential of malicious pdf files – but I have not heard a specific example. Other security-basics readers know of any?

I don't know about Chris's business, but there are plenty of Flash and RealPlayer marketing presentations, news, seminars, classes which managers and others will want to view. Even some material for Windows Media Player only.

I have not noticed much of an exploit history of Flash and Real products, but maybe they are not popular targets for the best analysts.

If many admins take the approach of Chris (which sounds reasonable) and end up with these products as helpers instead of plug-ins then web designers will have to be *\*much\** more careful when they embed links to these in javascript.

When you ban ActiveX, look at other (safer?) ways to enable pdf, and maybe rm and flash content and the revolt should be much smaller (but maybe the risk will be greater too :-))

Rejecting flash will make most portal sites load quicker – so hope that users thank you for that – distracting flash advertising is pervasive.

> >How will you stop them from loading ActiveX controls? There are ways  
> >(IEAK,  
> >Software Restriction Policies, registry edits), but it certainly won't be  
> >as  
> >easy as telling your user's not to do it.  
>  
> True, but no one said life as an Admin was easy.

> >Want to use another browser that doesn't  
> >accept ActiveX controls?  
>  
> Too unstandardized, wont' cover all situations.  
>

Don't brush this off too quick. Netscape and Mozilla will run on nearly every platform you have – and you can run the same version everywhere (good luck in standardizing IE across Mac, Windows and Solaris)

> >What about Java applets? Secure? Nope. Java's been hacked dozens of  
> >times.  
>

Re: Ten least secure programs

## SecurityFocus BASICS: Re: Ten least secure programs

> *Too pervasive, can't restrict it.*

I see fewer and fewer java applets each month. Probably because Windows does not have a VM installed by default.

Do the alternative VMs have a smaller exploit history than the one that is made available for IE?

I did not seem much in the bug reports for sandbox breakouts in IBM or Sun VMs in the last few years. Maybe I am reading the wrong bug reports but I feel ok with leaving Java applets enabled.

From this users' experience, disabling ActiveX seems to disable many Java applets on IE, so you may already have lost most of what you wanted to preserve. (I don't know javascript at all – but I suspect that this happens when the Java call is embedded in javascript – almost certainly happened with an online banking app – I wish I kept a list of these sites, but I tend just to go on to another one that works better.)

David

---

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant, while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

---