

# Re: Getting Fox News to work with Firefox

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Fedora/2007-01/msg03221.html>

---

- *From:* taharka <[res00v18@xxxxxxxxxxx](mailto:res00v18@xxxxxxxxxxx)>
  - *Date:* Mon, 22 Jan 2007 13:11:55 -0500
- 

How do,

On Mon, 2007-01-22 at 11:32 -0600, Les Mikesell wrote:

Dotan Cohen wrote:

- 2) They rely on AcitiveX, Java or some other dangerous script.

Can you elaborate on the dangers of java?

From the faqs at, <http://www.noscript.net/faq>

1.10

Q: Why should I allow JavaScript, Java and Flash execution only for trusted sites?

A: JavaScript, Java and Flash, even being very different technologies, do have one thing in common: they execute on your computer code coming from a remote site.

All the three implement some kind of sandbox model, limiting the activities remote code can perform: e.g., sandboxed code shouldn't read/write your local hard disk nor interact with the underlying operative system or external applications.

In the past, many security exploits have been based on "privilege escalation", i.e. exploiting an implementation error of the sandbox to acquire greater privileges and perform nasty task like installing a trojan.

This kind of attack can theoretically happen with JavaScript, Java and Flash, even their statistic scores are quite different:

1. JavaScript looks by far the most dangerous (most fixed vulnerabilities discovered to date were actually unexploitable if JS was disabled). Probably this is because it is easier to test and search for holes, even if you're a newbie hacker: everybody and his brother believe to be a JavaScript programmer :P
2. Java has a better history, at least in its "standard" incarnation

Re: Getting Fox News to work with Firefox

which is the Sun JVM.

There have been viruses, instead, written for the Microsoft JVM, like the ByteVerifier.Trojan. Anyway, the Java security model allows signed applets (applets whose integrity and origin are guaranteed by a digital certificate) to run with local privileges, i.e. just like they were regular installed applications. This, combined with the fact there are always users who, in front of a warning like "This applet is signed with a bad/fake certificate. You DON'T want to execute it! Are you so mad to execute it, instead? [Never!] [Nope] [No] [Maybe]", will search, find and hit the "Yes" button, recently caused some bad reputation even to Firefox (notice that the article is quite lame, but as you can imagine had much echo).

3. Flash have the shortest list of known security flaws, and they are pretty old. Nonetheless, such a list exists and this is enough to show that vulnerabilities are possible, even if unlikely.

4. Other plugins are harder to exploit, but they can still contain flaws like buffer overruns that may execute arbitrary code when feed with a specially crafted content (it happened with Windows Media Player, for instance).

Please notice that none of the forementioned technologies is usually (95% of the time) affected by known and unpatched holes, but the point of NoScript is just this: preventing exploitation of even unknown yet security holes, because when they are discovered it could be too late ;) The most effective way is disabling the potential threat on untrusted sites.

--  
Les Mikesell  
lesmikesell@xxxxxxxxxx

Hope the above helps :-)

taharka

Lexington, Kentucky U.S.A.

--  
fedora-list mailing list  
fedora-list@xxxxxxxxxx  
To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>