
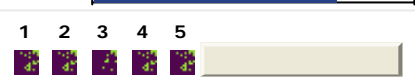


Web Browser Vulnerabilities: Is Safe Surfing Possible?

Date: Aug 05, 2004
Section: Articles :: Misc Network Security
Author: Deb Shinder
 [Printable Version](#)
Rating: 3.8/5 - 16 Votes

1 2 3 4 5



This article takes a look at what makes Web browsers vulnerable to malicious attackers, how popular Web browsers differ (or don't) in this regard, and what you can do to protect yourself when Web surfing, no matter which browser you choose.



There has been a lot of media attention recently regarding vulnerabilities in Microsoft's Internet Explorer Web browser – to the point that the U.S. government's Computer Emergency Readiness Team (CERT) issued a warning in June recommending that computer users stop using IE. What's up with that? Are you risking your life (or at least your data's life) by continuing to use Microsoft's Web browser? What are the critical issues and can they be addressed? Are other Web browsers as invulnerable as the headlines would make you believe?

The Web Can Be a Dangerous Place

Back in the "olden days" of the World Wide Web, "seeing the sites" was a relatively safe activity. Most Web pages were written in simple HTML, with text and pictures and not much else (of course, the very first browsers were text-only). An animated .gif was about as "active" as it got prior to the 90s. However, Web developers soon fell prey to the "gotta build a better mousetrap" syndrome, and all sorts of new technologies emerged to make Web browsing a richer, more entertaining and more interactive experience.

Soon Web pages contained much more than text and pictures. Web designers began to use scripting and other embedded code to make their pages come alive. Microsoft introduced ActiveX, an outgrowth of OLE and COM technologies, that provides functionality similar to Java applets but with more flexibility (and posing a bigger security risk) because ActiveX controls can access the Windows operating system.

Scripts, applets and ActiveX controls can all be embedded in Web pages to do some amazing things, but they can also be used by malicious coders to do not-so-wonderful things such as infecting your computer with a virus, surreptitiously install software on your machine that will allow a hacker to take control of it, launch an attack, etc. This is due to the nature of the technologies; like all technologies, it can be used for good or evil.

As if that weren't enough, all popular Web browsers (like all software of every type) have security flaws, some more serious than others. Microsoft's Internet Explorer has recently been hit by the discovery of several serious security holes, including the "download.ject" exploit that affects IE users when they access a Web site on an infected IIS machine.

Is IE the Problem?

CERT's recommendation (see <http://www.internetnews.com/security/article.php/3374931>) that users consider an alternative browser was based on the fact that so many security flaws have been found in IE. It seems as if a week doesn't go by without another one – or several – being announced. However, the recommendation overlooks the fact that during the same time period, vulnerabilities were also announced affecting the Mozilla and Opera Web browsers, two of the most popular alternatives to IE.

Anti-Microsoft advocates respond that the flaws in other browsers occur with less frequency, are less serious, and are patched more quickly. There is certainly some truth to their claims.

Internet Explorer has the largest share of the browser market by far, just as Windows has the largest share of the client operating system market. The "big guys" will always be the most popular target of hackers and critics alike. If creating malicious code or attacks is your "thing," why spend your time developing them for browsers or OSs that are only used by a relatively small portion of the computing public? It makes more sense to target the software

that's in most widespread use. That means as long as IE remains the most popular, it will be the most popular browser for which to search for holes and develop exploits. It also means that if CERT's and others' recommendations to switch browsers are taken seriously and another browser becomes the most popular, the bad guys will in all likelihood turn their attention to that browser and we'll see a surge in exploits for it.

What about the claim that the security flaws in IE are more dangerous than those found in other browsers? Because IE is much more closely integrated with the operating system, it's true that the potential is there to do more damage through it. This is especially true if you "open up" all the security restrictions when configuring your browser options. This is not an uncommon reaction of frustrated Web surfers who find that certain pages won't work with IE in a more secure configuration – so they just enable everything. Ouch! Microsoft gives you a lot of flexibility to configure your security settings, but you have to use common sense in setting those configurations or you'll put yourself at risk.

Do other browser makers get their patches out faster than Microsoft? Unfortunately, that's often true. Many of the companies that make other browsers are small companies with few or no other products. They can focus exclusively on the browser. The larger a company (or government, or any other entity) gets, the more slowly it tends to respond. In a small company, the management team (or a single person) can make the decision and get the new patch out within days or even hours. In a large company, such decisions have to wind their way through the bureaucracy, be commented on by the legal advisors, undergo testing and more testing, etc. In many ways, Microsoft is a victim of its own phenomenal success.

The bottom line: you probably *will* be more secure using one of the less popular browsers instead of IE, at least for the time being. This is particularly true for users who are less tech savvy and don't understand how to properly configure security settings. But does that mean everyone is going to stop using IE? We don't think so.

Why Users Will Continue to Use IE

A recent survey of readers of the WinXP News (www.winxpnews.com) indicated that despite CERT's recommendations, over half stated that they intend to stick with Internet Explorer, at least for some of their browsing activities. Reasons are varied. Humans tend to crave the familiar, and if IE is what they've been using for years, many would prefer not to switch and have to learn something new, regardless of how intuitive it might be. Humans also tend to be lazy. IE comes with the operating system, ready to use, and doesn't require that you download and install anything.

Some folks are "twice shy" after having a bad experience with an alternative browser. A few reported that the other browser wouldn't install, or worse, that it did install and "broke" other programs or caused their OS to crash. Still others have found that many Web sites are developed with IE in mind, and don't display or work properly with other browsers, at least not with the default settings. For example, the Web GUI for a firewall appliance I was testing last week couldn't be opened in either Mozilla or Opera with default settings; IE opened it with no problems.

The "best" browser interface is a matter of personal preference, and some people just like IE better. In the past, many stuck with IE because it was the only browser for which the Google toolbar was available, although it can now be installed on Mozilla and is even included with the Firefox edition of Mozilla's browser (<http://www.mozilla.org/products/firefox/>). For whatever reasons, many users will continue to browse with IE as long as it's available. The question is: what can they (and users of *all* browsers) do to make their surfing experience safer?

Safe Surfing Guidelines

Here are some guidelines that every Web user in your organization should be made aware of:

1. If there is sensitive data on your computer, don't browse the Web. In the business environment, computers that hold classified data should not be used for Web browsing, period. This helps to limit Web-based attacks to computers that don't contain the most sensitive data.
2. Install security patches and updates. Administrators tend to focus on operating system patches and may pay less attention to updates that are "only" for the Web browser. However, only download patches from known authorized sites. There have been cases of e-mail purporting to be from Microsoft containing fake patches that actually contained malicious code.
3. Ensure that browsers are of the latest version and capable of using the strongest (128 bit) encryption for secure communications.
4. Disable plug-ins and configure security settings not to run Java applets, JavaScript and VBScript, ActiveX controls, etc. without prompting you first. If you need to have a plug-in for a particular activity, enable it temporarily for that activity only, and then disable it again.

5. Consider using more than one Web browser, for different activities. For example, a recent IE exploit made it possible for hackers to collect information such as passwords typed into banking Web sites, via a software key logger. Although I prefer to use IE for general Web browsing, I took the precaution of using a different browser (even switching to a different computer, using Safari on Mac OS X) for financial transactions.

This last is something that few users seem to consider: there is no reason you have to commit to only one Web browser. I have IE, Firefox, Opera and Maxthon (formerly known as MyIE2) all installed and peacefully coexisting on my primary workstation. This helps me in developing my own Web sites, because I can check out how (and whether) various components work in alternative browsers (for instance, some of the Web components such as hover buttons that you can easily insert with FrontPage look great in IE, but don't translate to other browsers). More importantly, if I need to go to a site I don't know is trustworthy, I can do so with a browser that is less likely to be exploited.

Summary

It's up to network administrators to take the lead in educating users about the best security practices. While we *could* enforce policies requiring users to use an alternative browser, this might be only a temporary solution and in some cases, might not be feasible. We should also learn how to better secure *all* Web browsers and disseminate that information to the computer users in our organizations.

About Deb Shinder

Debra LittleJohn Shinder(MCSE) is a technology consultant, trainer and writer who has written a number of books on networking, including Computer Networking Essentials, published by Cisco Press and Scene of the Cybercrime, published by Syngress Media. She is co-author, with her husband Dr. Thomas Shinder, of Troubleshooting Windows 2000 TCP/IP and the best-selling Configuring ISA Server 2000, both published by Syngress Media, as well as the new ISA Server and Beyond. Deb tech edited Syngress's Security + Study Guide and was a major contributor to Que's TruSecure ICSA Certified Security Associate exam guide. Deb lives and works in the Dallas-Ft Worth area and can be contacted at deb@shinder.net or via the website at www.shinder.net.

