;login:

THE MAGAZINE OF USENIX & SAGE

February 2003 • volume 28 • number 1

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

web browser vulnerabilities 101

by Peleus G. Uhley

Peleus Uhley is the senior developer for Anonymizer Inc., where he is responsible for the privacy surfing service and privacy analysis "Snoop" page.

peleus@anonymizer.com

Recently, Microsoft Internet Explorer made the SANS/FBI Top 20 Security Vulnerabilities list.[1] For followers of BugTraq, you will have seen new postings of browser vulnerabilities monthly over the past year. For all the hype surrounding these issues, how is the browser a vulnerability? If you don't visit hacker sites, is there a threat? The answer is, sadly, yes in more instances then you might expect. This article focuses on Internet Explorer, but most of what is presented is true for any Web browser currently available.

To start, let's look at what it means to be a browser. Most people will answer with the most popular function, which is to transform the Hyper-Text Markup Language (HTML) into a viewable Web page. In the case of Internet Explorer, the browser can also interpret Java, ActiveX, JavaScript/JScript, VBScript, XML, XLST, and several other languages. Depending on the language, they may be compiled by the browser locally on the PC. The browser can launch almost any application, including media players and mail clients.

Internet Explorer is designed with the Microsoft Container-Object model, enabling you to view Word, Excel, and many other documents from within the IE container. The browser code overlaps with Windows' Explorer to access files on the Internet, in your network, and in your local file system. The browser can both send and receive files from the Internet. In addition, programs such as Outlook, Outlook Express, AOL, and MSN use the browser's internal engine to render HTML formatted email. The browser can use active content to have bi-directional communication between third-party software and itself.

Once you realize the full power of the browser, it becomes more apparent why it is such a targeted piece of software – it is the next best thing to hacking the OS itself! A recent WebSideStory report stated Internet Explorer is used by 95.97% of all Internet users.[2] The rate at which vulnerabilities are posted makes it very difficult for administrators and the general public to keep the browser patched at all times. In addition, Microsoft has not patched all the holes found within the browser! Although Microsoft was able to shorten the list of unpatched vulnerabilities from 31 down to 19 between November and December,[3] this has been a race they have been losing all year.[4]Add to this the fact that business and personal firewalls usually allow all outgoing port 80 traffic and you have a potentially high-risk situation for the personal workstation.

Types of Vulnerabilities

Vulnerabilities in Web browsers take many forms. The SANS/FBI report warns:

"The vulnerabilities can be categorized into multiple classes including Web page spoofing, ActiveX control vulnerabilities, Active scripting vulnerabilities, MIME-type and content-type misinterpretation and buffer overflows. The consequences may include disclosure of cookies, local files or data, execution of local programs, download and execution of arbitrary code or complete takeover of the vulnerable system."[5]

To give some definition to their classes and add examples, I provide the following general explanations with footnote references to specific examples.

Web page spoofing: In Web page spoofing the attacker makes you believe you are at a "safe" site when you are really at a site controlled by the hacker. These attacks can include altering IE's location bar to show the wrong URL, mixing real site content with

1. *http://www.sans.org/top20/* – SANS/FBI Top 20.
2. *http://www.Websidestory.com/cgi-bin/wss.cgi?corporate&news&press_1_193* – WebSideStory report on browser usage.
3. *http://www.pivx.com/larholm/unpatched/* – List of unpatched vulnerabilities.
4. *http://www.pivx.com/larholm/unpatched/archivednews.html* – History of IE vulnerabilities.
5. *http://www.sans.org/top20/#W8* — IE section of SANS/FBI Top 20.

altered content, and showing the title of the page being spoofed, making it almost impossible to determine that you are not where you think you are.[6]

ActiveX control vulnerabilities: Signed ActiveX controls run as resident programs on your PC with full privileges when loaded through IE. The operating system treats signed code as local code. By default, IE does not prompt the user about this action so long as the code is signed. If someone has access to a certificate, then this type of attack could be very transparent. For example, a malicious hacker could use this in order to load buggy DLLs signed by the original vendor to temporarily downgrade your computer.[7]

Active Scripting vulnerabilities: Although almost all of the attacks described use Active Scripting to operate; the scripting languages themselves can have vulnerabilities in their implementation within the browser. These usually lead to bypassing the Security Zone restrictions for local file access, program execution or Cross-Site Scripting (CSS) attacks.[8] Cross-Site Scripting is the ability for one site to gain access to another site's data such as their cookies or form information. Active Scripting attacks can involve JavaScript, JScript, VBScript, and XLSA. JavaScript is usually the language-of-choice for exploits.

Mime-type/Content-type vulnerabilities: Here the attacker falsely sends an incorrect file type in the headers to fool the user into downloading an executable. This could also be used to launch another application, such as a mail program to parse and run the active content outside of IE's restrictions.[9]

Buffer overflows: IE is just as vulnerable as the next program to this classic programming error. For IE, these can be infinite loops that crash the browser[10] or they can also be variable overflows.[110]

There are many ways to fool the user without using browser exploits. The Cuartango Window is the oldest example: Here a window with a harmless question such as, "Do you like chocolate?" covers a security window asking to run harmful code.[12] Users believe they are answering the chocolate question but the OS takes "yes" as the answer to whether to run the code. Another attack is to spoof the entire screen so that the user is no longer interacting with the OS![13]

Other recent problems include IE's SSL implementation allowing forged SSL connections through certificate chaining.[14] Some of Internet Explorer's default settings can also be a danger. By default, IE allows Web sites complete access to whatever information is currently copied onto your clipboard. In addition, many other programs interact with IE allowing for an attack through those programs.[15] There have been recent attacks against both Java[16] and IE's[17] compilers.

Almost all vulnerabilities reported to BugTraq include sample code (often only a few simple lines) making these attacks easy to implement.

Type of Threats

Some people may consider this a somewhat apocalyptic view. What if they only visit "safe" sites such as business and news sites? Most exploits require a person to visit an unsafe site to launch the exploit, so where is the problem? Browsers aren't always on servers and aren't always installed on servers so is there a corporate threat?

First of all, you have to remember that your Outlook mail clients and other pieces of software use IE's engine for rendering HTML-based email or connecting to the Net.

[6] *http://www.securitytracker.com/alerts/2001/Dec/1003024.html* – Web spoof.

[7] *http://www.guninski.com/signedactivex2.html* – Signed ActiveX of old DLLs.

[8] *http://security.greymagic.com/adv/gm010-ie/* – "Who Framed Internet Explorer?"; *http://security.greymagic.com/adv/gm012-ie/* – "Vulnerable Cached Objects in IE (9 Advisories in 1)."

[9] *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-020.asp* – Microsoft's posting regarding MIME vulnerabilities.

[10] *http://online.securityfocus.com/archive/1/269241* – Looped buffer overflow.

[11] *http://online.securityfocus.com/archive/1/289106* – Buffer overflow to code execution.

[12] *http://www.safenetworks.com/Windows/ie26.html* – Cuartango Window.

[13] *http://www.guninski.com/popspoof.html* – Spoofing entire screen.

[14] *http://online.securityfocus.com/archive/1/292842* – IE6 SSL certificate chain.

[15] *http://online.securityfocus.com/archive/1/282631* – ICQ and MSIE.

[16] *http://lists.netsys.com/pipermail/full-disclosure/2002-November/002730.html* - IE Java Vulnerabilities.

[17] *http://online.securityfocus.com/archive/1/301220* - Netscape Java Vulnerabilities

Internet Explorer is "an integrated part of the Microsoft operating system." Patching your browser can help reduce the risk of viruses and attacks through these other programs.

On the Internet, you would most likely have to visit an unsafe site. However, the line between safe and unsafe is getting more and more blurry. Recently, spam that tells users they have an e-greeting card has been used to lure people into visiting a Web site and having them accept an ActiveX control to send spam to everyone in their address book.[18] You should also consider the possibility of a worm or hackers altering your "safe" site and including one of these exploits. Worms, trojans, and viruses are becoming more sophisticated and are beginning to use a mix of Web and email for their distribution.

The SANS/FBI report looks at IE as being threatened from your internal Web administrators. Many businesses have internal use only Web pages that show statistical reporting, business memos, Web-based email, and other information deemed important to the business. Web site administrators could use the aforementioned exploits on these internal pages to grab the CEO's files, email authentication cookies, or other information directly from his machine without ever having logged into the victim's machine. Disgruntled employees with personal Web sites might easily be able to social engineer someone within the company into visiting an exploit page on their site as well.

Prosecution could be potentially difficult in these situations. The fact that there is no login and, in most attacks, no software installed makes it difficult to identify that there was ever even an attack. If the victim was visiting a trusted internal Web site, then the traffic won't stick out in most logs. By the time a problem is realized, the browser cache may already be overwritten and the malicious page would be changed back to normal. People may not even think to look at these vulnerabilities as an attack mode since they are not as commonly seen.

The Web browser is not a daemon server so a direct attack cannot be launched against it. Most browser attacks are more of a trap situation, where the attacker attempts to lure the user in or plants the trap somewhere the user is sure to go. This makes it great for targeting an individual or small group. If an attacker needs to do an active attack, they could target a server on their system that talks to the browser, such as an instant messaging client, and get that software to deliver the attack.

Types of Solutions

The prevalent use of Active Scripting on the Internet does not make disabling it in your browser an easily viable solution. Luckily, there are as many protections against these problems available as there are types of attacks. Each of the solutions has a different focus and should be looked at in terms of your corporate or personal needs.

Traditional free methods: You can frequently patch your systems, but not all problems are patchable, so this should not be considered a solution in and of itself. Patching and upgrading the browser should be as equally important as updating the OS. It would also be helpful to make sure your browser security settings match your policies. I would also recommend including surfing security as a part of your company's security education program.

Corporate solutions: Employee Internet Management (EIM) are corporate Web s filters, such as WebSense and Surf Control. These help to limit your employees to viewing traditionally safe and can block active content based on file type. Corporate

[18] *http://www.cnn.com/2002/TECH/ptech/10/28/security.net/index.html* – E-Mail Greeting Card Hides Porn.

content filters, such as Finjan's SurfinGate and Alladin's E-Safe offer software for your gateways to filter active content on both Web and email, which is a little more permissive then just blocking. Their design allows them to be combined with antivirus and EIM software to give well-rounded, continuous protection for your office. Finjan's SurfinGuard executes all code in a sandbox allowing you to fine-tune control of active content.

Mobile protection: Anonymous proxy systems such as a service-based Anonymizer can strip and/or filter active content that may be malicious. These have the added feature of masking any research your firm may be doing on the Web and adding encryption to prevent sniffing. Recent versions of personal firewalls such as Zone Alarm or Norton can be configured to block, warn against, or allow potentially harmful Web content. Desktop antivirus software can also pick up on some Web attacks that have been used in viruses.

Current Status

Every time that I hope they have found all the holes in IE, there are three more postings on BugTraq. In my opinion, Microsoft coupled their browser too tightly to the OS, and to software development related to the OS, to provide good security. This isn't to say other browsers are pristine. Microsoft is definitely not the only group struggling to deliver the full power of the Web securely. Mozilla, which is the basis for many browsers, has had its fair share of browser exploits as well. Mozilla-based browsers don't get as much media attention or hacker attention because of their lower usage. They report to have 9.6% of the market.[19] Even Lynx, which is a text-based Web browser for UNIX, has had security vulnerabilities.

Unfortunately, I don't believe any browser group will ever be able to deliver the complete power of the Web with complete security all on their own. The browser is expanding it's roles and responsibilities to handle more and more technologies. A study last year determined that the Linux 6.4.2 kernel had 2.4 million lines of code and that Mozilla had 2 million lines of code.[20] Considering that Mozilla is the basis for more sophisticated browsers such as Netscape, an advanced browser can exceed the size of the Linux kernel. Browsers are becoming increasingly powerful and complex.

Based on this, I believe that the number of exploits in browsers and the high degree of browser interaction with other software will continue at its current rate for some time. The expanding size and scope of the browser makes it a more and more tempting target. Viruses, trojans, and worms are increasingly using HTTP in addition to mail as their mode of delivery. It is only a matter of time before more scripts become widely available for the script kiddie community to exploit. Fortunately, most hackers who have found holes are currently content with proving the holes exist and not going further.

On the upside, every browser hole that is fixed is one less hole to be found and one more lesson learned by the browser community. The other browsers in the market need the same level of scrutiny as Microsoft. Hopefully, the other browser teams are watching what is going on with IE and reviewing their own code for the same problems.

Third-party vendors are still behind in handling the newer Web technologies. People need more of an option than just disabling active content. Although filters for scripting have come a long way, the industry is still lacking in filtering various media types.

[19] *http://www.infosecuritymag.com/2002/nov/digest07.shtml#news3*.
– Six Pack of Mozilla Vulnerabilities Discovered.

[20] *http://www.dwheeler.com/sloc/redhat71-v1/redhat71sloc.html*.
– More Than A Gigabuck: Estimating GNU/Linux Size.

The filters and sandboxes for these technologies need to be advanced and in some cases invented. It would be advantageous for the browser groups to work more closely with third-party vendors in helping to secure the content coming into the browser.

In addition, education of the general public on issues related to browser security will need to be improved. Along with touting more advanced features, browser groups should also emphasize the increases in security that come with the upgrades. There are too many technologies involved with the Web for the average user to comprehend each one, but they need to know there is protection out there and that they should be using it.

Conclusion

The important thing to remember for the corporation is that Web browsers are more than just a threat to your employees' productivity. You have to consider the threats from both outside and inside your business. Home users need to learn that their Web browser is as vulnerable as their mail clients. Due to the increasing importance of the Internet, Web browsers are evolving into mini-operating systems, and patching them should be taken as seriously as patching an OS. If an attack occurs, administrators will have trouble identifying the source of the attack since there are few clues left behind on the victim machine. Fortunately there is supplemental software and services available to protect against the large number of unpatched vulnerabilities in Internet Explorer that leave Windows exposed to an attack. It is sometimes hard to comprehend just how much of a threat Web surfing can be. After all, how much harm can a little Web page do?

RELATED LINKS

http://www.Websense.com – WebSense.

http://www.surfcontrol.com – Surf Control.

http://www.esafe.com – Alladin's E-Safe product.

http://www.finjan.com – Finjan Software.

http://www.anonymizer.com – Anonymizer.

http://www.zonelabs.com – Zone Labs (Maker of Zone Alarm).

http://www.symantec.com – Symantec.

http://www.anonymizer.com/snoop – Privacy analysis page.