

Web Browser Security Comparison: Internet Explorer vs. Firefox

An iDEFENSE Security Report

iDEFENSE Intelligence Operations
Sept. 30, 2005

TABLE OF CONTENTS

1	Introduction	2
2	Background.....	3
2.1	Microsoft Internet Explorer	3
2.2	Mozilla Firefox.....	4
2.3	Timeline.....	4
2.4	Key Functionality.....	5
2.4.1	Microsoft Internet Explorer	5
2.4.2	Mozilla Firefox	5
2.5	User Base	5
2.5.1	Microsoft Internet Explorer	5
2.5.2	Mozilla Firefox	6
3	Metrics.....	7
3.1	Total Vulnerabilities	7
3.2	Patching.....	8
3.2.1	Patch Status Statistics.....	8
3.2.2	Patch Time	9
4	Lab Tests.....	11
5	The Future	13
5.1	Microsoft Internet Explorer	13
5.2	Mozilla Firefox.....	13
5.3	Netscape.....	13
6	Recommendations.....	14
6.1	Interoperability.....	14
6.2	Security.....	14
6.2.1	Microsoft Internet Explorer	14
6.2.2	Mozilla Firefox	14
7	IE or Firefox?	15

1 Introduction

As the number of vulnerabilities in Microsoft Corp.'s Internet Explorer (IE) continues to climb, users are looking elsewhere for a safer Web browsing solution. Competing Web browser developers are taking advantage of IE's security shortcomings to gain market share on Microsoft. One such entity, The Mozilla Organization, has experienced great success with the release of its Firefox browser.

iDEFENSE analysis shows that the number of vulnerabilities in both IE and Firefox are climbing, and that malicious codes are taking advantage of these issues to infect and spread across the Internet. As these threats mount, users are left waiting for patches, updating anti-virus signatures, and continually looking for a more secure solution. Both Microsoft and Mozilla are taking measures to secure their respective products, each with mixed success. This paper will compare and contrast these two browsers and their respective futures from a security perspective.

2 Background

2.1 Microsoft Internet Explorer

Microsoft Corp.'s Internet Explorer (IE) is the proprietary Web browser, included in every version of Microsoft's operating system since Windows 95. In 1995, Microsoft licensed Mosaic, a browser originally owned by Spyglass Inc, to create IE.¹ This new browser broke into the market by providing features that Netscape, the leading Web browser at the time, lacked, such as Cascading Style Sheets (CSS) support. IE's core code has not been significantly updated for some time. The latest IE version, 6.0, was released in October 2001, which has resulted in gaps in compliance with new Web standards, such as the W3C CSS specifications.²

IE maintains the largest market share in the industry. This is largely due to the fact that IE is distributed with the popular Microsoft Windows operating systems. As a result, most users are familiar with IE because of its status as the default Web browser.

Microsoft became involved in an anti-trust case in 1998 for employing monopolistic practices. In the case, the US Department of Justice (DOJ), along with 20 state governments, alleged that Microsoft had abused its monopoly in the operating system market by building IE with Windows. Competing companies complained that Microsoft was tying two unrelated products together to prevent fair competition in the Web browser market. Microsoft argued that the integration of IE with Windows was the result of innovation, and that the two were essentially the same product. In 2000, the court reached a verdict, stating that Microsoft had indeed attempted to monopolize the market, and ordered that the company be split into two parts; one to develop the operating system, the other to develop other products.³

Microsoft appealed this decision, and it was overturned on the grounds that the judge had displayed a bias against Microsoft to the media. The Washington, DC circuit court found that Microsoft had abused its monopoly position, and remanded the case for further consideration. On Sept. 6, 2001, the DOJ announced that it was no longer going to attempt to split Microsoft as originally intended, but rather charge the company with a lesser anti-trust penalty. In November of that year, the DOJ settled the case with Microsoft. The settlement required the company to share its Application Programming Interfaces with third-party companies and appoint a panel of three people to ensure compliance with the verdict.

¹ http://en.wikipedia.org/wiki/Internet_explorer

² <http://www.positioniseverything.net/explorer.html>

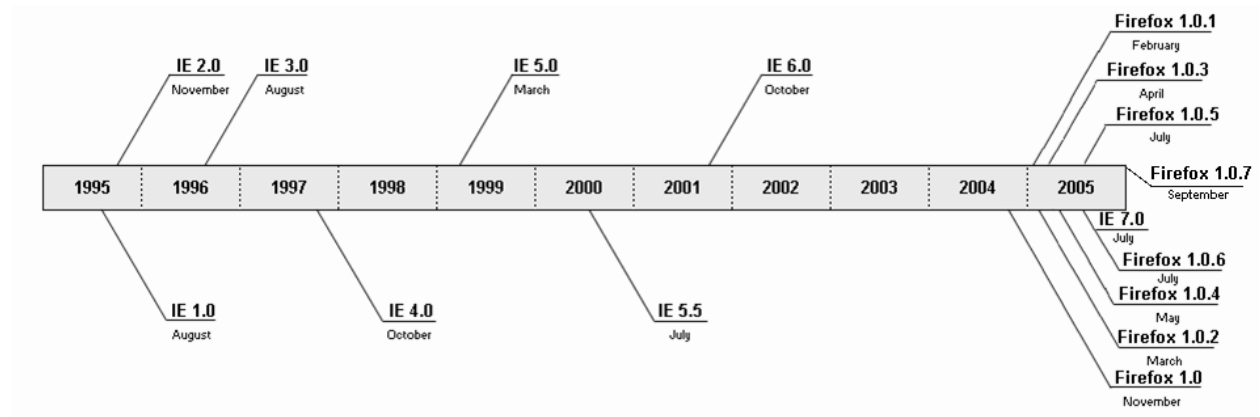
³ http://en.wikipedia.org/wiki/Microsoft_antitrust_case

2.2 Mozilla Firefox

Mozilla Firefox is the brainchild of The Mozilla Organization, a nonprofit entity established in July 2003 with help from America Online Inc.'s Netscape division. The Firefox project began when two developers from the Mozilla team set out to create a more streamlined version of the existing Mozilla browser. They believed that the Mozilla Suite contained too many unnecessary features, such as an Internet Relay Chat (IRC) client and a full-blown HTML editor⁴. Released on Nov. 9, 2004, Firefox was created as a free, open-source, cross-platform Web browser. Firefox's popularity continues to grow, with campaigns such as "Spread Firefox" that promote the browser.⁵

2.3 Timeline

As illustrated in the following timeline, IE maintained a steady release schedule from its debut in August 1995, until October 2001. Since then, IE development has stagnated, resulting in security gaps. Microsoft has chosen to address these security gaps by issuing updates and patches rather than developing a new version. However, Microsoft has shown recent progress toward releasing its newest browser with the release of a beta version of IE 7.0. This beta version was released exclusively to developers, however.



Web Browser Release Timeline⁶

Firefox, on the other hand, is relatively new to the field, with all major releases occurring within the past year. Respectively, Firefox is still in its infancy, leading many to theorize that, as Firefox's popularity grows and it becomes a more attractive target for security researchers, it may eventually face the same security issues that IE has experienced.

⁴ <http://en.wikipedia.org/wiki/Firefox>

⁵ <http://www.spreadfirefox.com/>

⁶ <http://www.blooberry.com/indexdot/history/browsers.htm>

2.4 Key Functionality

2.4.1 Microsoft Internet Explorer

IE is designed for ease of use; it takes advantage of the familiar look and feel of the Microsoft Windows environment. IE is a fundamental piece of software within Windows, and is integrated into many components of the operating system. For example, the Windows Update patching mechanism uses a Component Object Model⁷ technology, called ActiveX, to interact with the host computer. The crucial Windows Update service would not work without IE, leaving systems unable to be easily secured against emerging threats. The *Lab Tests* portion of this report details the decrease in functionality when IE is completely decoupled from the operating system.

2.4.2 Mozilla Firefox

The main features of Firefox include tabbed browsing, pop-up blocking, a built-in search toolbar and a collection of themes and extensions. Extensions are small additions to Firefox that can be installed to add different features. Many of the extensions available on the Firefox website were written by users attempting to add some form of desired but previously unavailable functionality. There are currently 661 free extensions available online.⁸ The most popular extensions include FlashGot, a download manager; Adblock, an advertisement-thwarting tool; and Forecastfox, an extension to keep users updated on the local weather. Other extensions are available to extend security and privacy functionality, such as an anti-virus scanner, a Cookie Manager, a Script Blocker and a Password Generator.

Extensions are easy to develop, as Firefox is an open-source product with freely available tools and documents for developers. This is one of the primary differences between IE and Firefox. The open-source model allows anyone to review and improve upon the code. The open-source model also makes porting the browser to different platforms easier. To date, Firefox has been ported to Windows, Linux, Mac OS X, Solaris and OS/2.

2.5 User Base

2.5.1 Microsoft Internet Explorer

IE currently holds the largest market share in the browser industry with 88.46 percent.⁹ The browser has been bundled with Microsoft's Windows operating system since 1995; users likely choose IE because it is familiar and because it does not require any installation or setup to use. Many large corporate environments may have Internet Explorer as their designated browser. In addition, the browser implements many of the same features available with Windows, such as the accessibility framework, which aids people with disabilities.¹⁰

⁷ <http://www.microsoft.com/com/default.msp>

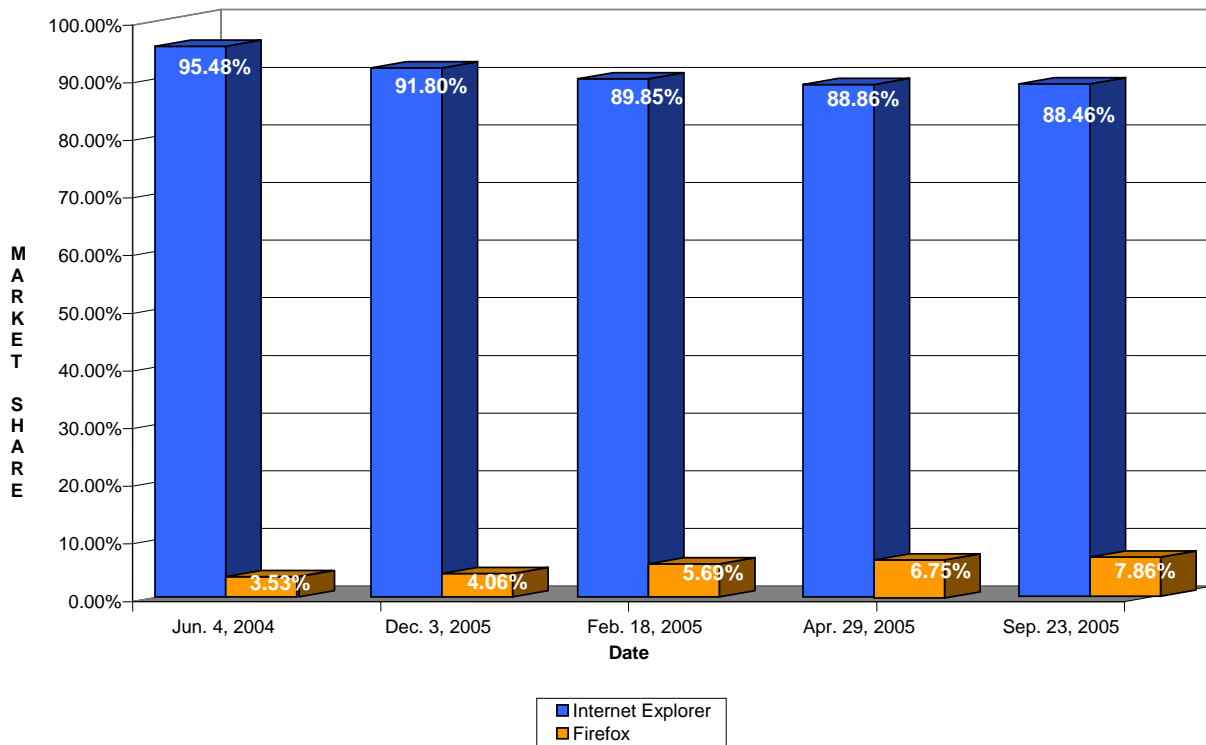
⁸ <https://addons.mozilla.org/extensions/?application=firefox>

⁹ http://blogs.websidestory.com/datainsights/2005/09/firefox_cools_down_1.php

¹⁰ <http://www.microsoft.com/enable/microsoft/history.aspx>

2.5.2 Mozilla Firefox

The Firefox Web browser, as an alternative to Microsoft's IE, is quickly gaining popularity and market share. Firefox runs on many operating systems and has been embraced by the open-source community. In light of prominent new IE vulnerabilities, an increasing number of users have switched to Firefox. According to WebSideStory, an online Web analytics company, Firefox now holds 7.86 percent market share as of September 2005.¹¹ The following graph illustrates how Firefox has slowly gained in popularity since its release in November 2004.



Browser Market Share Trends
(data from WebSideStory)

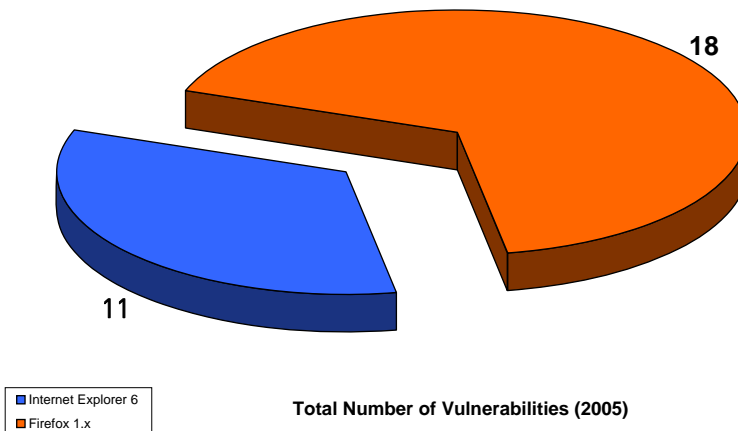
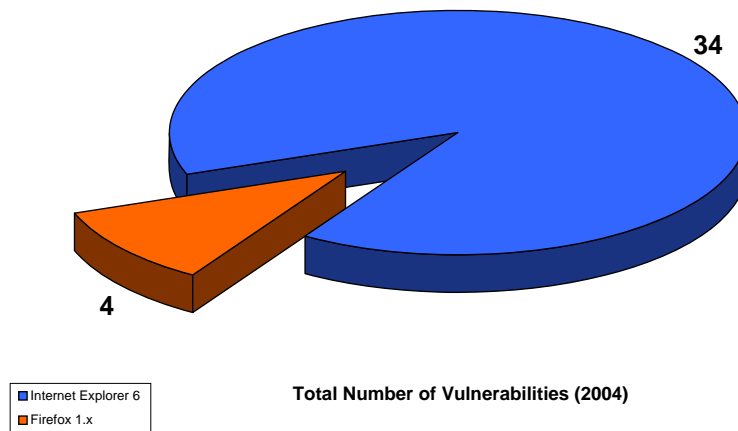
It should be noted that the data for June 2004 in this graph includes usage statistics for all Mozilla-based browsers, as Firefox was not tracked separately at the time.

¹¹ http://blogs.websidestory.com/datainsights/2005/09/firefox_cools_down_1.php

3 Metrics

3.1 Total Vulnerabilities

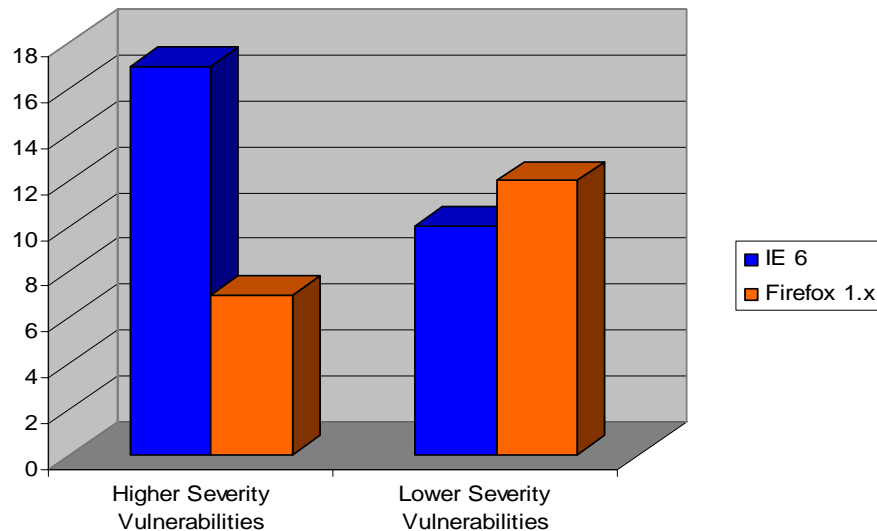
The total number and frequency of vulnerabilities are important statistics when analyzing a product's security. The following graphs show the total number of vulnerabilities released for IE and Firefox in 2004 and 2005. As the following graph illustrates, the number of year-to-date IE vulnerabilities reported has decreased. This could be the result of the many security enhancements implemented with Service Pack 2. The number of reported Firefox vulnerabilities, on the other hand, has been increasing. This is most likely because Firefox is increasingly being scrutinized by security researchers.



These vulnerabilities should be dissected further when comparing the security of the two products. Specifically, the severity of exploitation on a given system should be considered. A vulnerability that causes a denial of service condition, rendering the system or browser useless until a reboot or restart, is much less threatening than a vulnerability that could result in code execution, root-level or user-level access to the system. Of the vulnerabilities in IE, 17 could result in some sort of system access that may allow code execution or user- or root-level access. Only seven vulnerabilities in Firefox could result in such consequences. This equals 38 percent of Microsoft's total vulnerabilities and 32 percent of Firefox's total vulnerabilities, which is not much of a difference. Firefox seems to be more susceptible to the minor

vulnerabilities that result in spoofing or denial of service conditions. Firefox was subject to 12 of these vulnerabilities, as opposed to 10 by Microsoft; 55 and 22 percent of total vulnerabilities, respectively.

Vulnerability Severity Comparison



Researchers have been searching for vulnerabilities in IE for some time, so Firefox is quickly becoming a new target. Furthermore, Microsoft has become notorious for security issues. To address this, Microsoft more thoroughly patches IE. Note that the 2005 data covers vulnerabilities announced through early September.^{12 13}

3.2 Patching

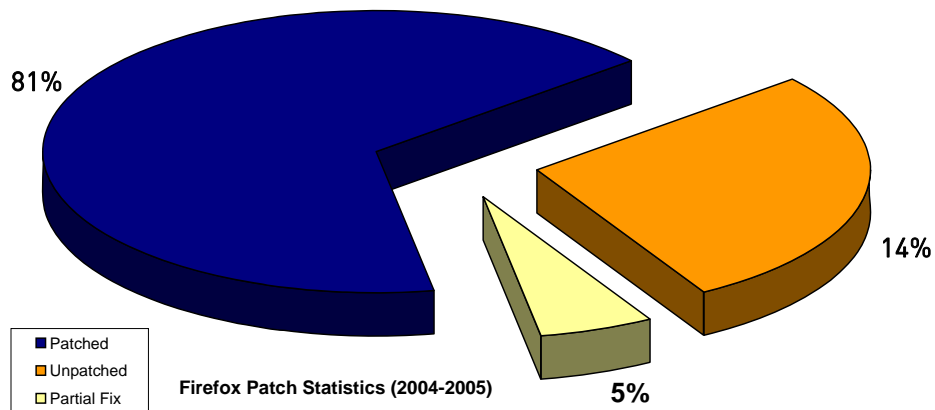
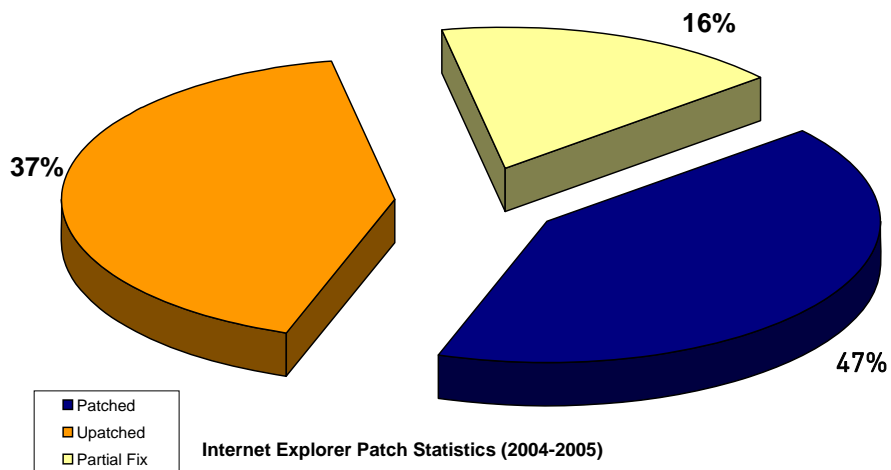
3.2.1 Patch Status Statistics

Microsoft and Mozilla have each taken different approaches to address vulnerabilities in IE and Firefox. Mozilla tends to release a new version of the product, including a number of security fixes and functionality changes. These releases come relatively quickly and have averaged 1.5 months since the initial release of Firefox on Nov. 9, 2004. Microsoft, however, generally releases a patch designed to fix a specific vulnerability or series of vulnerabilities. Both vendors have automated functionality to manage the patching process. Microsoft uses a feature called Windows Update that automatically queries Microsoft's server for updates and installs them; this application can be scheduled to run at specified times. Firefox has a Software Update feature built into the Options dialog. It automatically checks for and installs updates for the browser and the accompanying extensions and themes.

The amount of time it takes for a vendor to release a fix is an important statistic because it determines how long users are vulnerable to a publicly known issue. The following charts illustrate the status of patched, unpatched and partially fixed vulnerabilities to date in Firefox and IE; they include issues disclosed in both 2004 and 2005. Many of the unpatched vulnerabilities may be mitigated by disabling features, such as Active Scripting, and the vendor has therefore not released an official patch.

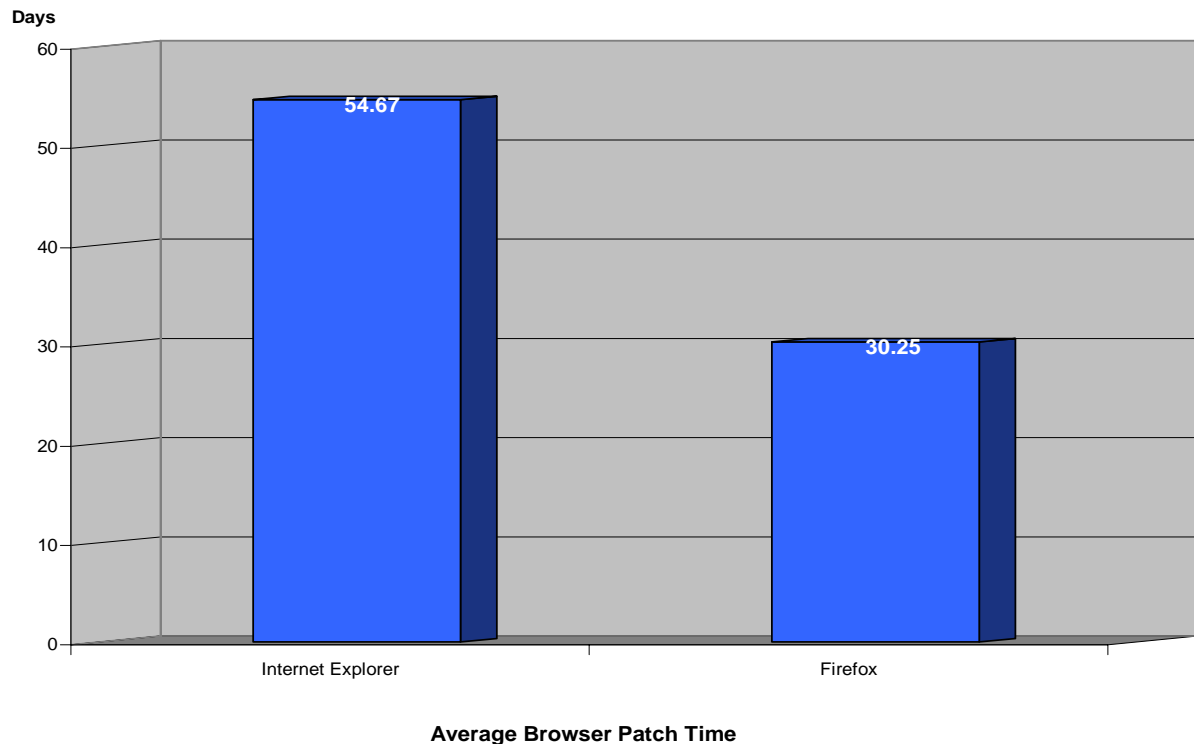
¹² <http://secunia.com/product/11/>

¹³ <http://secunia.com/product/4227/>



3.2.2 Patch Time

One of the more important vulnerability-related aspects of software is the time that it takes for a vendor to patch a recently discovered issue. From the time a vulnerability is announced publicly, exploitation may be possible until a patch or workaround is issued. This introduces the possibility of users being susceptible to exploitation for that amount of time. The following graph illustrates the average number of days it takes to release a patch once a vulnerability is announced for IE and Firefox between 2004 and 2005.



As this graph illustrates, Firefox currently has a quicker turn-around period between vulnerability disclosure and subsequent patch release. This is an important factor when choosing a browser because it projects the potential window of opportunity for malicious attackers to take advantage of "zero-day" vulnerabilities.

It should be noted, that Microsoft has a set schedule to release updates on the second Tuesday of each month. Further, if a patch is not functional or does not pass testing benchmarks, Microsoft will hold off on releasing that particular update. This happened in September 2005. Microsoft was preparing to release a patch, but then canceled its bulletin release once the patch was found to have failed several tests. These factors are detrimental to patch time and should be noted when analyzing the above graph.

To Microsoft's credit, in the event that the company foresees an immediate risk, it will presumably release an immediate (but temporary and usually simplistic) patch to mitigate the problem until a fully tested update may be released.

The data in the above graph does not include vulnerabilities released by the vendors themselves. It only addresses situations where vulnerability details were released before a vendor patch was made available.^{14 15}

¹⁴ <http://secunia.com/product/11/>

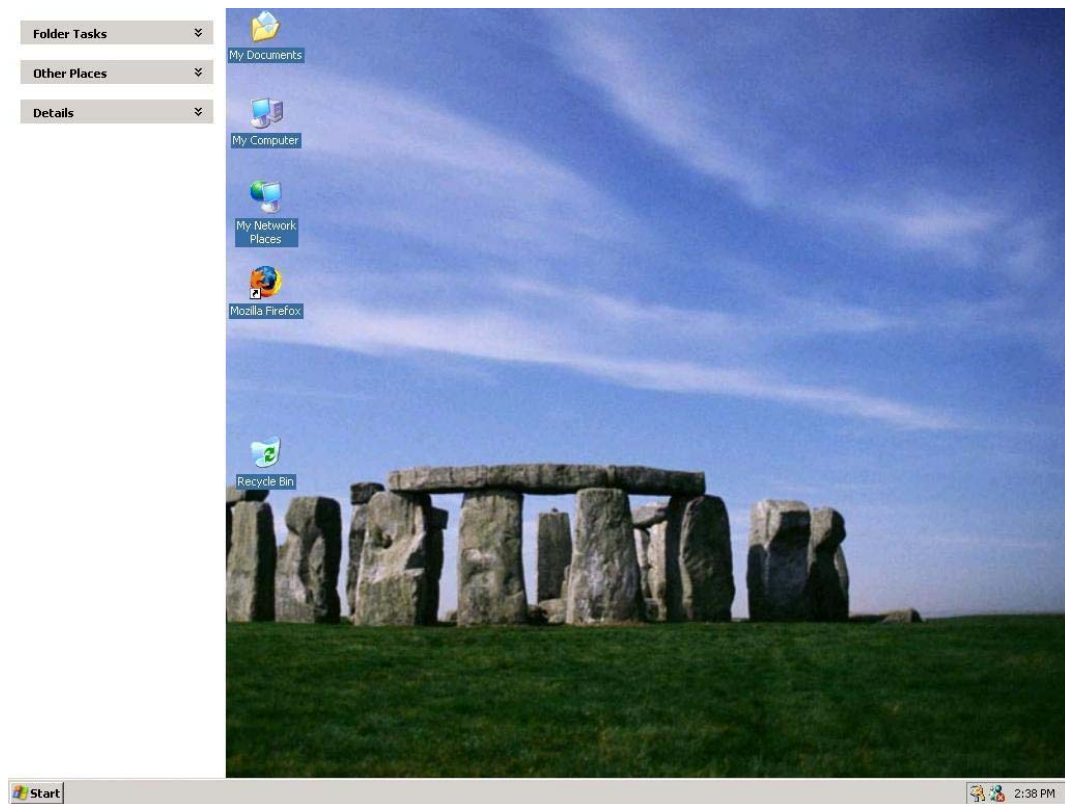
¹⁵ <http://secunia.com/product/4227/>

4 Lab Tests

To better understand the operating system's dependency on IE, iDEFENSE Labs removed IE from a default installation of Windows XP. Decoupling the browser from any Windows version after 98 is a complex and poorly documented process. Following unofficial directions obtained from an online forum post, all instances of IE functionality were removed.¹⁶ This was performed to better ascertain the true level of integration between the Windows operating system and the IE Web browser.

The decoupling process was far from straightforward. It involved booting from a floppy disk and removing numerous Dynamic Link Library (DLL) and executable files. It is important to note that simply removing IE through the Add/Remove Applications program in the Control Panel merely removes shortcuts to the browser from the desktop and Start menu; it does not permanently remove any components of IE.

The most noticeable change after the process was completed was the appearance of the desktop. Upon a reboot of Windows, the interface in the following screenshot is overlaid on the desktop:



Windows XP without IE Desktop Screenshot

This screenshot shows what appears to be the left navigation menu that is available when an instance of Explorer is browsing the file system.

¹⁶ http://www.ntcompatible.com/How_to_completely_remove_Internet_Explorer_6_from_XP_system_t23510.html

iDEFENSE lab tests show that the following features of Windows fail to work properly when IE is removed:

- *Windows Update*
- *Device Manager*
- *Remote Assistance*
- *Help and Support*
- *All Troubleshooting Wizards*
- *Activate Windows*
- *Disk Defragmenter*
- *Disk Backup*
- *Program Compatibility Wizard*
- *Address Book*
- *Search For People*
- *Windows Media Player*
- *Windows Catalog*
- *Hearts and Spider Solitaire*
- *Internet Games (Checkers, Backgammon, Hearts, etc.)*

As shown, key functionality is broken when IE is removed. For example, some of these applications are critical to the security of the computer, such as Windows Update and the Device Manager. These applications may have failed because the DLL files that handle Web connectivity through IE were removed with the browser. Certain DLL files were restored to see if this was indeed the case; however, this further distorted the desktop, but did restore some functionality in select applications. This demonstrates the deep level of integration between IE and the operating system. Because of this, iDEFENSE recommends that users not attempt to remove IE from Windows.

5 The Future

5.1 Microsoft Internet Explorer

On Feb. 15, 2005, Bill Gates, Chairman of Microsoft Corp., announced the planned release of Internet Explorer 7.¹⁷ Microsoft has reportedly redesigned the underlying security infrastructure of IE in this latest version. Specifically, Gates announced that IE 7 will contain improved capabilities for blocking malicious code and thwarting phishing and spoofing attempts. IE 7 also reportedly includes new features, such as tabbed browsing and better Web support for standards. This version is being touted as the response to the multitude of vulnerabilities that have recently inflicted IE, and an attempt to regain users who have switched to alternative browsers. In summer 2005, Microsoft released a beta version of IE 7 exclusively for developers. Initial feedback from iDEFENSE customers who have been briefed on IE 7 has been very positive.

Unfortunately, many users are worried that the new IE will not support Windows 2000. Microsoft has been debating the logistics of whether to remain portable to 2000 and delay the release of the new version, or to support only XP. It is likely that they will not be supporting any Windows version other than XP, but Microsoft has yet to state so publicly. Many companies still use Windows 2000, and are reluctant to make the switch to Windows XP. Assuming that IE does not support 2000, users running Windows 2000 will be left with the less-secure IE 6.

5.2 Mozilla Firefox

Mozilla is currently in the alpha stages of development on Firefox 1.1, codenamed "Deer Park." Mozilla has reportedly improved upon the Gecko engine that the browser uses, added a new feature to report broken websites, and made changes to the extension system.¹⁸ In addition, Mozilla has implemented an interface to the Microsoft Outlook e-mail client, whereby users can receive "new mail" notifications and launch a new Outlook composition window. This alpha version is freely available online for download, and is being reviewed by the Firefox user community. Unlike Microsoft, which distributes beta versions to chosen testers, Mozilla uses an online bug-reporting system to which any user may post issues that they encounter. The reported bugs are all displayed and tracked on the Mozilla Bugzilla system and are reviewed by fellow users and the Mozilla team.¹⁹

5.3 Netscape

Netscape Communications Corp. has recently released a new version of its Netscape Browser. Version 8.0 incorporates both the Firefox Gecko browser and Internet Explorer. Netscape automatically switches to the browser that is more suitable to the page being viewed. It also includes features such as tabbed browsing, many new security enhancements and customizable menu bars. Because Netscape has less than one percent share of the browser market today, iDEFENSE has elected not to cover it in this report. Should Netscape dramatically gain in market share, iDEFENSE will revisit this research.

¹⁷ <http://www.microsoft.com/presspass/press/2005/feb05/02-15RSA05KeynotePR.asp>

¹⁸ <http://weblogs.mozillazine.org/asa/archives/008197.html>

¹⁹ <https://bugzilla.mozilla.org/>

6 Recommendations

6.1 Interoperability

Organizations that are not running Windows XP should strongly consider deploying an alternative browser. When it released IE security fixes in XP Service Pack 2, Microsoft hinted that it will no longer support IE on any system but XP, and that there will be no updates for any other Windows version. If upgrading to Windows XP is not an option, users will be forced to use IE 6, leaving them subject to its inherent security issues.

If an alternative browser is to be deployed, IE should still remain on the system, as it is so closely integrated that removing it would severely degrade the functionality of Windows. If an organization is looking to deploy an alternative browsing solution, Firefox is a reasonable choice. It operates well on all supported platforms, including Windows. The only major issues that have arisen regarding its interoperability are the fact that it cannot utilize ActiveX, and that it reportedly runs slower because it is not as integrated with the operating system.²⁰ Users have also reported that Firefox does not correctly render many Web pages. This is due to the fact that most pages are designed with IE in mind, and will render with higher quality using Microsoft's browser.

6.2 Security

6.2.1 Microsoft Internet Explorer

With the release of IE 7, Microsoft will have reportedly addressed many of the security issues it has been plagued by recently. If an organization runs Windows XP as their main platform, IE 7 will be a much needed upgrade. Assuming that IE 7 fulfills the security needs of its users, a switch to an alternative browser will most likely not be necessary for a corporate environment running XP. However, if Windows 2000 or earlier is still in use, the switch to an alternative browser should be considered.

6.2.2 Mozilla Firefox

Firefox is still in its infancy, and as more users begin to migrate to it, it will become more widely scrutinized by the security industry. In the future, this may lead to the discovery of more vulnerabilities within, and more malicious codes targeting, the Firefox browser. As of this writing, Firefox is not being widely targeted by malicious code, and is therefore a safer solution than IE from a malicious code perspective.

As time progresses, and as Firefox gains more market share, malicious code is likely to surface that targets Firefox specifically. However, at this time, it does not seem worth the effort for malicious code authors to exploit Firefox as they endeavor to infect the larger user base currently held by IE.

²⁰ <http://www.techsupportalert.com/firefox.htm>

7 IE or Firefox?

Until Firefox gains even more market share, it cannot threaten Microsoft's browser. The downside of popularity, however, is increased attention, resulting in more known vulnerabilities and malicious codes targeting them.

While Firefox continues to rise in popularity, it has yet to be tested as extensively as Microsoft. Internet Explorer is a critical component of the Windows Operating System and has already proven its ability to withstand malicious scrutiny.

Although, Firefox seems to be an up and coming safe alternative to Internet Explorer, the Windows OS could not do without its' native browser. The functionality its' presence provides is sometimes one of necessity. However, including Firefox on desktops for alternative browsing may be a wise security shift.

From a threat perspective, it seems obvious that, as long as Internet Explorer maintains its firm grip on the market, we can expect the majority of new malicious code to make it the top target. For this reason, Firefox should be considered a reliable alternative, but will need to be monitored closely for increased scrutiny, with regard to security.