certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0077

Securing Web Browsers

Original Issue Date: December 14, 2016

Description

The web browser is a software application used for viewing and interacting with world wide web(www) information resources(URL/URI), such as web page, text, graphics, video, music, games etc. Internet Explorer/Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, and Apple's Safari are the most prevalent of the web browsers, primarily used for accessing the Internet websites, can be also used to view files in the local file systems and to access the information provided by the web-server in the private networks.

The default web browser that is provided with an operating system is not set up in a secure configuration, but to optimize the user's browsing experience. Therefore securing the web browser becomes necessary in order to prevent against the software attacks that can lead from spyware being unknowingly installed to hackers causing the complete system-compromise.

Some specific features that affect the web-browser's functionality and the system's security are discussed in brief:

1. **ActiveX**

   ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or otherwise it can be automatically downloaded and executed by a Web browser. ActiveX is a set of rules for how applications should share information. Programmers can develop ActiveX controls in a variety of languages, including C, C++, Visual Basic, and Java.They have full access to the Windows operating system imposing severe security risks if not properly implemented.

   Prevention: ActiveX Filtering in Internet Explorer prevents sites from installing and using these malicious ActiveX control apps.

2. **Java**

   The Java development platform provides a system to develop active content for websites. A Java Virtual Machine, or JVM, is used to execute the Java code, or "applet" provided by the website. Some operating systems come with a JVM where it is available to browsers as a plug-in, while others require a JVM to be installed before Java can be used. Java applets are operating system independent and are generally untrusted, come from unknown sources, and are launched automatically by the browser when directed by a website. Java applets usually execute within a "sandbox" where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute.

   Prevention against Java-in-the-browser risks:

   It has become very important for the user to limit Java applets executing from within the browser, however there are also web applications that still rely on Java availability from within the browser, so completely removing it is not always an option, especially in corporate environments where internal applications may rely on it. Different ways of mitigation:

   - Disable Java in the Browser
   - Use a Separate Browser for Java-based Web Applications

   Multiple browsers installed on the same system can increase security by designating one browser to have Java enabled while the others are used as general-purpose browsers with Java disabled. The Java-enabled browser should only be used for sites that require Java, such as internal corporate applications, and be restricted from external browsing.

   - Update the Browser's Java version

3. **Plug-ins**

   Plug-ins and extensions are applications that enhances the functionalities and features generally not already available in the browsers. Some of the more familiar plug-ins include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, Real One Player, and Acrobat Reader. Based on a web page's design, specific plug-ins may be required to view some content. These Plug-ins can contain programming flaws such as buffer overflows, or other design flaws such as cross-domain violations, which arises when the same origin policy is bypassed.

   Precautions:
   - Use caution when installing browser plugins: There is the possibility of a few of plugins being fake or unreliable. Before installing any plug-ins, check the reputation and ratings on several different rating websites and read customer reviews about them, use the knowledge that is out there on the web to help ensure getting quality plug-ins that will not harm browser and computer.
   - Download and install trusted security plug-ins for browser: Installing trusted and reliable security plug-ins for browser will keep user safe from having

to search for privacy and security settings in browser which will save time and keep the user just as secure.

4. **Cookies**

   Cookies are files placed on the user's system to store data for specific websites. A cookie can contain any information that a website is designed to place in it. Cookies may contain information about the sites visited by the user, or may even contain credentials for accessing the website. Cookies are designed to be readable only by the website that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached. Cookies can be used to uniquely identify visitors of a website, which some people consider a violation of privacy. If a website uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie.

   Managing cookies in browser:

   In browser settings, user can set up rules to manage cookies on a site-by-site basis, giving him more fine-grained control over privacy. This implies that he can disallow cookies from all sites except those that he trust. Browser contains an option to Clear Browsing Data which can be used to delete cookies and other site and plug-in data, including data stored on the user's device by the Adobe Flash Player (commonly known as Flash cookies).Users can browse in "incognito mode" or "private browsing mode" when the users do not want their website visits or downloads to be recorded in their browsing and download histories. Any cookies created while in incognito mode are deleted after all incognito windows are closed.

5. **JavaScript and VBScript**

   JavaScript is sometimes confused with Java, even though it is a completely different technology. JavaScript is a scripting language that runs within the browser and can interact with the elements on the web page that delivered it. VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in websites because of limited compatibility with other browsers.JavaScript and VBScript play an important role with drive-by malware delivery because these scripting languages are frequently leveraged to obfuscate the loading of malicious Java jar files, PDF, flash, or other components with flaws that are automatically loaded by a browser.

   The browser's capability to run scripting engine also enables web-authors to significantly add interactivity to their designed web-pages, but this is abused by attackers. The default configuration for most web browsers has scripting support enabled which can introduce multiple vulnerabilities, such as the following:

   - **Cross-Site Scripting(XSS):** Cross-site scripting is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.Cross-Site Scripting is not usually caused by a failure in the web browser. The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for the visitor. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker.

   - **Cross-Zone and Cross-Domain Vulnerabilities:**Although, most web browsers employ security models, primarily based on the Netscape Same Origin Policy, to prevent script in a website from accessing data in a different domain, vulnerabilities violating these security models can be exploited to cause cross-site scripting impacts or execute arbitrary commands on the vulnerable system when the attacker manages to cross into the local machine zone or other protected areas.

   Prevention against JavaScript-based malicious content download: To protect JavaScript tricks to foist malicious software and exploits onto site visitors, it is critically important to have an easy method of selecting which sites should be allowed to run JavaScript in the browser. Disallowing JavaScript by default and selectively enabling it for specific sites remains a much safer option than letting all sites run JavaScript unrestricted all the time.

   Threats/Attacks:

   1. **Drive-By Download web-browser attacks**

      Cyber-criminals use this attack methodology to exploit vulnerabilities in one of the modules composing the browser (HTML rendering, CSS parser, image parsers, JavaScript engine, etc.)or vulnerabilities in the browser plugins or extensions to perform malicious actions like allowing the execution of arbitrary binary code in the browser at the time when a user visits a compromised website, download of malicious payloads leading to data-exfiltration etc. The attacker can compromise a legitimate site, or can compromise advertising networks or can simply run a malicious phishing campaign to share links to a compromised website hosting the exploit kits.

   2. **Browser hijacking**

      The cyber-criminal take control of a computer's Internet browser in "Browser hijacking" attack and change format and content of what is displayed when the victim is surfing the Web, causing unauthorised modification of the browser's settings, damaging Windows registry settings, injecting malicious ads, hindering navigation to certain Web pages, such as antispyware and other security software sites, or causing installation of unwanted toolbars or Favorites, sometimes incurring permanent consequences.

Best Practices:

- Keep the browsers up to date .
- Enable click-to-play plug-ins, uninstall plug-ins that are not needed, keep plug-ins updated.
- Enable automatic updates for your browser.
- Block pop-ups, plug-ins and phishing sites.
- Set the browser not to store passwords.

- Disable third-party cookies.
- Keep the system up to date.
- Configure browser security and privacy settings.
- Use both anti-virus and anti-spyware software- Using both an anti-virus and an anti-malware program is critical to the security of not only browser but entire computer as well.
- Avoid fake security warnings: There are a whole host of fake security alerts that can start running and appear legitimate but if they are clicked they will infect the browser and computer with all kinds of malware and viruses. That is why it is critical to be up to date on these fake security warnings and know exactly what the real security alerts look like so that it can be avoided to click the fake ones and exposing your browser and computer to harm.

References

https://heimdalsecurity.com/blog/biggest-threat-in-your-browser/
https://instasafe.com/web/wp-content/uploads/2016/04/Instasafe-Definitive-Guide-to-Browser-Security.pdf
http://www.darkreading.com/risk/10-web-based-attacks-targeting-your-end-users/d/d-id/1140224?
http://www.cisco.com/c/en/us/about/security-center/java-best-practices.html#3

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India