ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

ضرورت امن سازی مرورگر وب

تنظیم کننده:

صابر نوروزپورلاری

ویرایش: ۱

شماره سند: T-89/5-3

www.ircert.cc

چکیده:

امروزه مرورگرهای وب یکی از ابزارهای بسیار پرطرفدار و پر استفاده می باشند. به دلیل آسان بودن نفوذ مهاجمان به اینگونه نرم افزارها بسیاری از این مرورگرها در معرض آسیب هایی از سوی مهاجمان می باشند که باید راه حلی برای آنها پیدا کرد در این مقاله ما شما را با یک سری ترفندهایی آشنا می کنیم که بتوانید از سیستم خود در برابر این آسیب ها محافظت کنید.

واژه های کلیدی:

web browser security، security ، internet explorer, browser setting

آپا ؟؟؟

مقدمه

این مقاله به شما کمک می کند تا گشت و گذار امن در اینترنت را تجربه کنید.

این مقاله برای کاربران رایانه های خانگی، دانش آموزان و کارگران کارهای کوچک و هر کسی که از پشتیبانی فناوری اطلاعات محدود برخوردار است و از DSL ، مودم های کابلی و یا حتی dial up استفاده می کند نوشته شده است.

همچنین اطلاعات این مقاله ممکن است برای کاربرانی که از پشتیبانی IT رسمی مثل پلیس IT سازمان ها استفاده می کنند نیز کاربرد داشته باشد. اگر شما مسئول IT سازمان خود هستید لطفا مطالب زیر را برای حفظ امنیت مد نظر قرار دهید.

چرا مرورگرها را امن کنیم:

امروزه مرورگرهای وب مثل Internet Explorer، Mozilla FireFox و Apple Safari، تقریبا بر روی تمام رایانه ها نصب شده اند. به خاطر اینکه در روز دفعات زیادی از مرورگر وب استفاده می شود، امن کردن آن یک امر حیاتی است. اغلب مرورگر های وب که همراه با سیستم عامل نصب می شوند تنظیمات پیش فرضی که امن باشد را ندارند. امن نبودن مرورگر وب باعث ایجاد مشکلات متعددی ناشی از جاسوس افزارهایی که بدون اطلاع کاربر بر روی سیتم نصب شده اند می شود، و باعث می شود تا کنترل رایانه مختل شود.

کاربران رایانه باید خطرات ناشی از نرم افزارهایی که استفاده می کنند را بدانند. بیشتر رایانه ها با نرم افزارهای نصب شده روی آنها خریداری شده اند، حال چه توسط شرکت سازنده رایانه، سازنده سیستم عامل و شرکت خدمات دهنده اینترنت نصب شده باشند و یا یک فروشگاه کوچک آن را روی سیستم

شما نصب کرده باشد. همچنین بررسی تقابل بین یک برنامه با دیگر برنامه ها را باید شناخت. متاسفانه اکثر مردم این سطح آنالیز را انجام نمی دهند.

تهدیدات زیادی از جانب نرم افزارهای مهاجم که از آسیب پذیری مرورگر وب استفاده می کنند وجود دارد. تمایل زیادی به استفاده از آسیب پذیری نرم افزارهای جدید در حین استفاده از بعضی وب سایت ها مشاهده شده است. که این مشکل با فاکتورهای زیر بدتر می شود:

۱- بیشتر کاربران تمایل دارند تا بر روی لینک ها بدون توجه به خطرات آن کلیک کنند.

۲- آدرس صفحه وبی که می خواهید از آن بازدید کنید ممکن است در حین اجرا عوض شود و شما را به یک سایت ناخواسته ببرد.

۳- بیشتر مرورگرهای وب برای کارایی بیشتر طوری ساخته شده اند که امنیت کمتری دارند.

۴- ممکن است آسیب پذیری های امنیتی بیشتری وقتی که نرم افزار توسط تولید کننده نهایی شد کشف شود.

۵-ممکن است سیستم ها و بسته های نرم افزاری با یک سری نرم افزارهای اضافی همراه باشد که باعث افزایش آسیب پذیری می شود.

۶-ممکن است نرم افزار مکانیزمی برای دریافت بروزرسانی امنیتی نداشته باشد.

- بعضی از سایت ها نیاز دارند کاربر یک سری مشخصه ها را فعال کند یا نرم افزارهای بیشتری نصب کند، که باعث می شود رایانه با یک سری خطرات جدید روبرو شود.

۸-بیشتر کاربرها نمی دانند چگونه می توان مرورگر وب را امن کرد.

۹- بیشتر کاربران تمایلی به فعال و یا غیر فعال کردن مشخصه های خاص برای افزایش امنیت ندارند.

بنابراین استفاده از آسیب ها در مرورگرهای وب یکی از روش های معمول برای مهاجمان سیستم های رایانه می باشد.

مشخصه های مرورگر وب و خطرات آنها:

آشنایی با ویژگی ها و کارایی های مرورگرها برای استفاده از آنها مهم است. فعال کردن بعضی مشخصه های مرورگر ممکن است امنیت آن را کاهش دهد.

اغلب فروشنده ها تنظیمات پیش فرض را برای مرورگرها انتخاب می کنند که این کار باعث افزایش آسیب پذیری سیستم می شود.

مهاجمان اغلب از بین آسیب پذیری ها ، آسیب رساندن به سیستم کاربر را انتخاب می کنند. آنها از این کار برای در اختیار گرفتن رایانه و آسیب رساندن به فایل ها، دزدیدن اطلاعات و استفاده از آن برای حمله به رایانه های دیگر استفاده می کنند. برای این کار یک راه کم هزینه وجود دارد که آن هم استفاده از آسیب پذیری مرورگرهای وب می باشد. یک مهاجم می تواند صفحه وبی بسازد و با ورود کاربر به آن نرم افزار تروجان و یا جاسوس افزار بر روی سیستم کاربر نصب کند و اطلاعات را بدزدد.

اطلاعات تکمیلی درباره جاسوس افزارها در لینک

http://www.cert.org/archive/pdf/spyware2005.pdf قرار دارد.

یک وب سایت مخرب به محض ورود کاربر می تواند سیستم را به خطر بیاندازد. حتی می توان یک فایل HTML برای قربانیان ارسال کرد که در این حالت باز کردن پست الکترونیک یا فایل پیوست سیستم را آلوده می کند.

در ادامه برخی ویژگی های خاص مرورگرهای وب وخطرات ناشی از آنها توضیح داده شده است. آشنا شدن با این ویژگی ها در امن کردن سیستم به شما کمک می کند.

Active X : نمونه ای از تکنولوژی مورد استفاده در Microsoft Internet Explorer در سیستم های دارای Microsoft Windows می باشد. Active X به برنامه های کاربردی و یا بخشی از برنامه های کاربردی اجازه استفاده از مرورگر را می دهد. یک صفحه وب می تواند از مولفه های Active X موجود در سیستم استفاده کند و یا اینکه ممکن است مولفه ها را به عنوان یک فایل قابل دانلود برای کاربر فراهم کند.

حتی اگر Active X برای استفاده در مرورگر وب طراحی نشده باشد ممکن است آسیب هایی به سیستم وارد کند. تحقیقات نشان می دهد که بیشتر آسیب ها مربوط به Active X می باشد که منجر به آسیب های جبران ناپذیری برسیستم می شود. در این موارد مهاجم می تواند کنترل سیستم را در دست بگیرد.

جاوا یک زبان برنامه نویسی مقصود گرا (موضوعی) است که می تواند برای توسعه محتویات متحرک وب سایت ها مورد استقاده قرار گیرد.

یک ماشین مجازی جاوا (JVM) ، که برای اجرای کدهای جاوا یا برنامه کاربردی applet استفاده می شود، توسط وب سایت ها فراهم می شود. برخی از آنها نیاز دارند که برای استفاده از جاوا، JVM نصب شود. برنامه java applet مستقل از نوع سیستم عامل بر روی همه آنها کار می کند.

Java applet ها معمولا وقتی کار با سیستم محدود باشد، توسط sandbox ها اجرا می شوند. هر چند پیاده سازی های مختلف jvm ها باعث آسیب هایی می شود که به برنامه کاربردی applet اجازه گذر از

این محدودیت ها را می دهد. برخی java appletها می توانند از محدودیت های sandbox هم عبور کنند اما آنها معمولا قبل از اجرا از کاربر اجازه می گیرند.

Plug-in ها برنامه های کاربردی مورد استفاده در مرورگرهای وب هستند. نرم افزار Netscape، استاندارد NPAPI را برای توسعه Plug-in ها در نظر گرفته است اما این استاندارد برای چندین مرورگر وب از جمله Mozilla firefox و safari استفاده می شود.

Plug-in ها شبیه active X ها هستند اما نمی توانند بیرون از مرورگر اجرا شوند.

Cookie ها فایل هایی هستند که برای ذخیره کردن اطلاعات از سایت هایی خاص در سیستم شما قرار دارند. یک Cookie شامل هر اطلاعاتی است که برای طراحی یک وب سایت نیاز می باشد. Cookie ها شامل اطلاعاتی درباره سایت هایی که بازدید کرده اید و یا حتی ممکن است شامل رمزهایی که برای دسترسی به یک سایت استفاده کرده اید باشد. Cookie ها طوری طراحی شده اند که تنها قابل خواندن توسط سایت سازنده آن باشند. Session Cookie ها (غیر ماندگار) وقتی مرورگر بسته می شود پاک می شوند و persistent cookie ها (ماندگار در سیستم) تا زمانی که تاریخ انقضای تعریف شده برای آنها برسد در رایانه باقی می مانند. Cookie ها می توانند کسانی که از یک سایت دیدن کرده اند را مشخص نمایند. اگر وب سایتی از Cookie ها برای تایید کاربر استفاده کند، آنگاه یک مهاجم با استفاده از همین Cookie ها می تواند بدون اجازه وارد سایت شود. Persistent cookie ها نسبت به Session cookie ها به خاطر اینکه بر روی رایانه باقی می مانند خطر بیشتری برای سیستم دارند.

Java Script ، که به اسم ECMA script هم شناخته می شود، یک زبان برنامه نویسی تحت وب است. استاندارد java script خصوصیاتی دارد که برخی ویژگی ها ازجمله دسترسی به فایل های محلی را محدود می کند.

script ، یکی دیگر از زبان های برنامه نویسی تحت وب است که فقط برای Microsoft Windows Internet Explorer استفاده می شود. VB script شبیه java script است اما به خاطر سازگار نبودن با دیگر مرورگرها استفاده چندانی ندارد.

توانایی اجرای زبانهایی ازجمله java و VB به طراح صفحه وب امکان اضافه کردن برخی ویژگی ها را به صفحه وب می دهد هرچند چنین قابلیتی باعث بیشتر شدن آسیب ها می شود.

تنظیمات پیش فرض اکثر مرورگرها پشتیبانی از scripting است که باعث ایجاد برخی آسیب ها از جمله موارد زیر می شود.

- Cross-site scripting که اغلب به آن XSS می گویند. یک آسیب پذیری در وب سایت می باشد که به مهاجمان اجازه نفوذ در ارتباط شما با یک وب سایت را می دهد.
- آسیب پذیری cross-domain و cross-zone

اکثر مرورگر های وب مدل های امنیتی برای جلوگیری از دسترسی Script ها به اطلاعات موجود در domain ها مختلف دارند. این مدل های امنیتی اصولا از قوانین netscape پیروی می کنند. Internet explorer هم قوانینی برای تفکیک ناحیه های امنیتی دارد.

می توان از آسیب پذیری هایی که مدل های امنیتی را مختل می کنند برای انجام کارهایی که یک سایت به طور معمول نمی تواند انجام دهد استفاده کرد. اثرات این کار می تواند شبیه

آسیب های XSS باشد. هر چند اگر یک آسیب پذیری اجازه ورود به نواحی محافظت شده بدهد، مهاجم امکان اجرای دستورات دلخواه را بر روی سیستم آسیب دیده خواهد داشت.

- شناسایی استراق سمع: یک ضد ویروس سیستم تشخیص ورورد غیر مجاز (IDS) و سیستم جلوگیری از ورود غیر مجاز (IPS) دارد که معمولا با جستجوی الگوهای مشخصی در محتویات

- سیستم کار خود را انجام می دهند. اگر یک الگوی ناشناخته شناسایی شد آنگاه برای محافظت از کاربر عملیات لازم انجام می شود. اما به خاطر طبیعت متغیر زبان های برنامه نویسی برنامه نویسی تحت وب برای گریز از چنین سیستم های محافظی استفاده می شود.

مرکز آپای دانشگاه شیراز

منابع:

http://www.microsoft.com/windows/ie/using/howto/security/setup.mspx

http://support.microsoft.com/?kbid=182569

http://www.us-cert.gov/cas/tips/ST04-022.html

http://www.us-cert.gov/cas/tips/ST05-001.html

http://www.us-cert.gov/cas/tips/ST04-012.html

http://www.cert.org/tech_tips/home_networks.html

http://www.cert.org/homeusers/HomeComputerSecurity/

http://www.cert.org/archive/pdf/spyware2005.pdf

http://www.cert.org/reports/activeX_report.pdf

http://www.opera.com/support/tutorials/security

http://www.mozilla.org/projects/seamonkey

http://www.konqueror.org

http://browser.netscape.com

مرکز آپای دانشگاه شیراز