کروم گوگل، میزبان چندین آسیب پذیری

باگ های متعددی در مرورگر کروم شناسایی شده است. هکرهای ریموت با استفاده از این بستر تخریبی می توانند کدهای دلخواه خود را بر رایانه های آسیب پذیر اجرا نموده و همچنین تدابیر به کار رفته در نرم افزارهای مسدود کننده پنجره های تبلیغاتی پاپ آپ (pop up blocker) را بی اثر سازند. به گزارش مهران رایانه به نقل از SecurityTracker، این باگ ها نسخه های پیش از ۱۰/۰/۶۴۸/۱۲۷ کروم را تحت تاثیر قرار می دهد.

Google Chrome

یاداور می شود کروم مرورگر تولید شرکت گوگل است که به طور رایگان عرضه می شود. این مرورگر سبک با زبان های برنامه‌نویسی سی++ و اسمبلی نوشته شده است. *(منبع: SecurityTracker)*

ضعف امنیت در گوشی های آندرویدی

اطلاعات تلفن های همراهی که در آنها سیستم عامل آندروید نصب شده است، به شدت در معرض خطر شنود قرار دارد. به گزارش مهران رایانه به نقل از سایت خبری رجیستر، سیستم عامل آندروید نمی تواند داده هایی را که از تلفن همراه به سایت فیس بوک و تقویم گوگل (Google Calendar) وارد می شود و یا از این دو سایت به گوشی داخل می گردد، رمزگذاری نماید.

این بدان معناست که حریم شخصی و خصوصی صدها میلیون کاربر آندروید در معرض تهدید و خطر است. آقای دن والاچ (Dan Wallach) استاد دانشگاه رایس این موضوع را عنوان کرده است.

بر اساس این گزارش یک سخنگوی گوگل با ارسال ایمیلی، از قصد گوگل برای رمزگذاری کردن ترافیکی که از آندروید به تقویم گوگل وارد می شود خبر داد. وی گفت که گوگل این کار را با ارائه یک وصله انجام خواهد داد اما زمان دقیق آن را اعلام نکرد. سخنگوی گوگل همچنین به کاربران توصیه کرد در صورت امکان از شبکه های رمزنگاری شده وای-فای استفاده کنند. *(منبع: Register)*

دانشجویان و دانش آموزان قربانیان جدید حملات فیشینگ

به نظر می رسد ایمیل های edu. چشم فیشرها را به خود جلب کرده است. به گزارش مهران رایانه به نقل از eSecurityPlanet، پژوهش های جدید موسسه امنیتی M86Security در کالیفرنیا حاکی از آن است که مقدار نامتعارفی از فریبکاری های فیشینگ، دانش آموزان مدارس را هدف گرفته است.

در این حملات فیشینگ یک صفحه اینترنتی مشاهده می شود که در آن اطلاعات شخصی کاربر از جمله نام خانوادگی، آدرس ایمیل، نام کاربری و کلمه عبور وی درخواست می گردد. سایت سافت پدیا مدعی است این صفحه توسط ابزار خودکار تهیه و طراحی شده است. به نظر می رسد این بزهکاری سایبری تاکنون توانسته تعداد زیادی قربانی را به دام اندازد.

یاداور می شود فیشینگ به تلاش برای سرقت و دستیابی به اطلاعات حساس افراد به وسیله جا زدن خود به جای یک وب سایت معتبر اطلاق می گردد. *(منبع: eSecurityPlanet به نقل از Softpedia)*

سخنان کارشناسان امنیتی در سبیت ۲۰۱۱

نمایشگاه بین‌المللی سبیت امسال با حضور صدها شرکت رایانه‌ای به مدت پنج روز در هانوور آلمان برگزار شد.

امسال در کنفرانس جهانی سبیت موسوم به CGC کارشناسان و فعالان عرصه امنیت IT به ابراز عقاید و ایده‌های خود پرداختند. به گزارش مشورت به نقل از ایتنا، ادی ویلمز یکی از کارشناسان امنیتی شرکت جی‌دیتا که در زمینه تولید نرم‌افزارهای امنیتی فعالیت دارد، در این کنفرانس گفته است: آموزش مهم است، همه ما ساده و بی‌تجربه‌ایم.

یواخیم شاپر معاون تحقیقاتی شرکت AGT Germany نیز در سخنانی اظهار داشت: مردم باید امنیت را جدی بگیرند. ما می‌توانیم در حوزه فنی کارهای زیادی انجام دهیم ولی کاربران با انتخاب یک کلمه عبور ضعیف، در معرض خطر قرار می‌گیرند. ریچارد مارکو مدیر عامل شرکت ایست نیز بر لزوم هوشیاری بیشتر کاربران در تعامل با محیط ابری

سخن گفت. جورج راو از شرکت دویچه پست، یکی دیگر از سخنرانان این کنفرانس بود. این کارشناس آلمانی بر ضرورت وضوح و شفافیت در سرویس‌های ابری تاکید کرد.

یاداور می شود نمایشگاه سبیت که هر ساله در شهر هانوفر آلمان برگزار می‌گردد، به عرضه فناوری‌های نوین می‌پردازد. این رویداد بزرگ امسال از اول تا پنجم مارس (دهم تا چهاردهم اسفند) برگزار شد. افتتاحیه این نمایشگاه با حضور آنجلا مرکل صدر اعظم آلمان و رجب طیب اردوغان نخست وزیر ترکیه و دیگر مقامات بلند پایه این دوکشور برگزار شد. CeBIT.de سایت رسمی نمایشگاه سبیت است.

بی‌توجهی شرکت‌های تجاری به امنیت اطلاعات کاربران

بر اساس مطالعه جدید انجام شده، اطلاعات شخصی که در اختیار شرکت‌های تجاری قرار می‌گیرد ایمنی لازم را ندارد و می‌تواند مشکلات عدیده‌ای را برای صاحبان این اطلاعات به وجود آورد.

بررسی جدید انجام شده توسط موسسه Imperva و Ponemon بر ۵۰۰ شرکت حاکی از آن است که حدود ۵۵ درصد از تمام شرکت‌های تجاری از برقراری ایمنی برای اطلاعات مربوط به کارت‌های اعتباری مطمئن هستند و در عین حال، هیچ گونه ایمنی برای شماره‌های امنیت اجتماعی، جزئیات اطلاعات حساب‌های بانکی و دیگر اطلاعات شخصی در نظر نگرفته‌اند.

این بررسی به منظور مشخص کردن میزان استفاده شرکت‌ها از "استاندارد امنیت اطلاعات مربوط به صنعت کارت‌های اعتباری" (PCI DSS) انجام شد. این استاندارد به منظور ایجاد امنیت لازم در سایت‌های اینترنتی شرکت‌ها، پایگاه‌های داده و دیگر سیستم‌های پردازش و ذخیره‌سازی اطلاعات شخصی کاربران تعریف شده است.

طبق مطالعه حاضر، ۷۱ درصد شرکت‌های تجاری ایمنی اطلاعات را اولویت اصلی خود نمی‌دانند و این در حالی است که ۷۹ درصد این شرکت‌ها اعلام کرده‌اند که پیش‌تر یک یا چند بار مورد حملات سارقان اینترنتی برای دسترسی به این اطلاعات قرار گرفته‌اند. *(منبع: ال نت)*

نگرانی کارشناسان از تروجان جدید "تاتانگا "

محققان امنیتی در حال تجزیه و تحلیل تروجان خطرناک و جدیدی هستند که برای کاربران اینترنت و وب نگرانی های جدی به وجود آورده است. این تروجان با نفوذ به حساب های کاربری مشترکان خدمات بانکداری و تجارت الکترونیک تلاش می کند اطلاعات حساس آنها را به سرقت برده و سپس از این اطلاعات برای انتقال غیرقانونی وجه و همین طور پولشویی استفاده کند.

تروجان مزبور که تاتانگا نام دارد از ابزار پیشرفته ای برای سرقت کلمات عبور در زمان تایپ آنها استفاده می کند. حمله به سرویس های بانکداری الکترونیک، سرقت اطلاعات حساس و حتی تصویربرداری از صفحه رایانه برای جاسوسی از دیگر اقدامات این تروجان است. تلاش برای شناسایی عوامل طراحی این تروجان کماکان ادامه دارد. *(منبع: ال نت)*

دو وصله امنیتی برای Wireshark

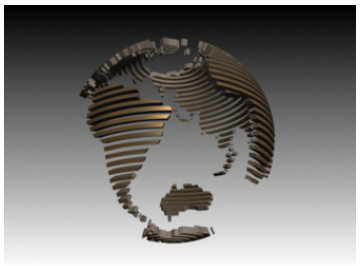
اخیراً نسخه های ۱/۲/۱۵ و ۱/۴/۴ نرم افزار Wireshark منتشر شد و در معرض استفاده عموم قرار گرفت. به گزارش مهران رایانه به نقل از eSecurityPlanet، این نسخه ها که در واقع به روزرسانی های ترمیمی هستند، دو باگ بسیار خطرناک موجود در Wireshark را رفع و رجوع می کند.

باگ اول عملکردی دارد که ممکن است به هنگام خواندن یک فایل pcap. در فرمت pcap-ng، اشکال در حافظه (memory corruption) بروز نماید. یک هکر ریموت می تواند با بهره گیری از این راهکار مخرب، حملات عدم سرویس دهی را راه اندازی کند. باگ دوم هم بالقوه می تواند به سرریز بافر از نوع پشته (heap-based buffer overflow) منجر شود. این امر به هنگام خواندن برخی فایل های خاص و آلوده Nokia DCT3 صورت می پذیرد.

یاداور می شود Wireshark یک ابزار آنالیز و اشکال زدایی پروتوکل های شبکه هاست که به طور رایگان در اختیار عموم قرار دارد. این نرم افزار متن باز بوده و به زبان C نوشته شده است. *(منبع: eSecurityPlanet)*

برخی عناوین اخبار IT
به نقل از خبرگزاری‌ها و سایت‌های داخلی

- **هشت برابر شدن تعداد حفره‌های امنیتی تلفن همراه** – ایستنا به نقل از ایسنا
- **چاپگرها به امکانات امنیتی مجهز می‌شوند** – فارس
- **تروجان زئوس به جان گوشی‌های بلک‌بری افتاد** – فارس
- **به روزرسانی فایرفاکس برای رفع ۱۰ حفره امنیتی** – ایستنا به نقل از فارس
- **وزیرارتباطات خبر داد: افزایش ۱۰۰ برابری پهنای باند برای کاربران موجود** – ایرنا
- **۴۰ درصد مردم سر رایانه خود داد می زنند!** – مدیانیوز به نقل از خبرگزاری مهر
- **محاسبه عددی امنیت سیستم‌های کامپیوتری** – ایتنا به نقل از خبرگزاری مهر
- **مایکروسافت: به خاطر امنیت هم که شده از IE6 استفاده نکنید!** – sgnec.net
- **کاهش آلودگی بدافزاری و هرزنامه در ماه فوریه** – ایسنا
- **وزیر ارتباطات: باید به شبکه فیبرنوری مهاجرت کنیم** – تلنا
- **۸۰ درصد پول رایج کشور الکترونیکی می‌شود** – مدیانیوز
- **عرضه رایانه‌های ارزان در انگلیس برای کاهش شکاف دیجیتال** – فارس
- **وزارت اقتصاد فرانسه آماج حملات سایبری** – ایسنا
- **آنچه در نمایشگاه سبیت ۲۰۱۱ گذشت** – ICTPRESS
- **تقی پور خبر داد: رشد ۳۰ درصدي بودجه وزارت ارتباطات در لایحه بودجه** – ایلنا



برخی عناوین اخبار IT
به نقل از خبرگزاری‌ها و سایت‌های خارجی

- حمله هکرهای آنونیموس به **BREIN** – eSecurityPlanet
- حملات عدم سرویس دهی علیه **WordPress.com** – Help Net Security
- گزارش یک باگ در **VMware ESX** – SecurityTracker
- حساب توییتری اشتون کوچر هک شد – eSecurityPlanet
- نسخه ۳/۶ نرم افزار **Metasploit** منتشر شد – Help Net Security
- شناسایی یک باگ در **Novell Vibe OnPrem** – SecurityTracker
- پادشاه هرزنامه نویس ها دوباره از زندان آزاد شد – Help Net Security
- پنج راه برای ایمن سازی **SaaS** – InformationWeek
- راهکارهایی برای تامین امنیت «مجازی سازی» – InformationWeek
- **KingSoft WebShield**؛ تروجانی که در دل نرم افزارهای امنیتی معتبر و قانونی مخفی می شود – SecurityProNews

- *نظرات، انتقادات و پیشنهادهای شما برای ما ارزشمند است: support@MehranCo.com*
- *آدرس کامل منابع اخبار، در «پشتیبانی فنی شرکت مهندسی مهران رایانه» موجود است.*
- *وب سایت رسمی شرکت مهندسی مهران رایانه، www.MehranCo.com می باشد.*
- *استفاده از اخبار و مطالب خبرنامه «با ذکر منبع» بلامانع است.*