شماره بیستم - شهریور ۱۳۹۷

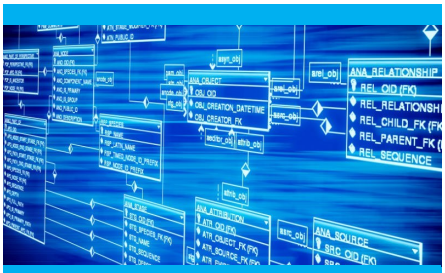
خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

به گزارش Avast، هزاران خانه‌ی هوشمند در هند در معرض نشت اطلاعات قرار دارند.

یکی از اخباری که در ماه جاری با توجه به رشد سریع وسایل IoT باعث نگرانی کاربران در هند شد، خبر نشت اطلاعات این وسایل محبوب در هندوستان است.
هرچند که استفاده از این ابزار در تمامی کشورهای جهان، کیفیت زندگی و آسایش را افزایش داده است اما تاثیرات آسیب پذیری هم نیز داشته است. - صفحه ۲



کشف آسیب پذیری روز صفر توسط تیم Trend Micro در موتور Jet مدیریت پایگاه داده‌ای مایکروسافت.

یک آسیب پذیری که قابلیت اجرای کد از راه دور را به مهاجمان می‌دهد در موتور پایگاه داده‌ای Jet مایکروسافت توسط تیم Trend Micro به تازگی کشف گردید. این باگ که در تمامی نسخه‌های ویندوز حتی windows server موجود است از زمان طراحی و پیاده سازی آن، همچنان مرتفع نگردیده است. - صفحه ۳

nuuo
The Intelligent Surveillance Solution

هکرها با استفاده از آسیب پذیری Peekaboo قادر به سرقت فیلم‌های مربوط به دوربین‌های نظارتی شدند.

یکی از وسایلی که عموما در اتصال با اینترنت قرار دارد و می‌توان به آن از هر جایی دسترسی داشت دوربین‌های مدار بسته و نظارتی می‌باشد. از این رو این وسایل نظارتی که عموما در مکان‌های مهمی هم قرار دارند می‌توانند خطرهای جدی را ایجاد نمایند. - صفحه ۴

باگ مرورگر کروم به هکر ها اجازه میدهد تا اطلاعات شخصی فیسبوک و دیگر پلتفرم‌های وب را استخراج کنند!

یک اشکال جدید کروم به مهاجمین اجازه می دهد اطلاعات خصوصی را که در فیس بوک و سایر پلتفرم های وب ذخیره شده‌اند را استخراج کنند. - صفحه ۵

نشت ۱۵۷ گیگ اطلاعات!

این بار پای هکرها به شرکت‌های خودروسازی باز شد و توانست حجم بالایی از اطلاعات حساس مربوط به شرکت‌های مطرح خودرو سازی در جهان را به دست آورند. ۱۵۷ گیگابایت اطلاعات حساس شرکت‌های بزرگی مثل تویوتا و فورد و تسلا به صورت آنلاین نشت پیدا کرد و در دسترس عموم قرار گرفت. - صفحه ۶

آسیب پذیری روز صفر در مرورگر Tor ورژن ۷

تیم Zerodium با انتشار توییتی از آسیب پذیری روز صفر در آخرین ورژن از مرورگر Tor خبر داد. این مرورگر دارای یک آسیب پذیری جدی می‌باشد که یک درب پشتی با قابلیت دور زدن تمامی تدابیر امنیتی مرورگر Tor است. - صفحه ۷

به گزارش Avast، هزاران خانه‌ی هوشمند در هند در معرض نشت اطلاعات قرار دارند.

یکی از اخباری که در ماه جاری با توجه به رشد سریع وسایل IoT باعث نگرانی کاربران در هند شد، خبر نشت اطلاعات این وسایل محبوب در هندوستان است.

هرچند که استفاده از این ابزار در تمامی کشورهای جهان، کیفیت زندگی و آسایش را افزایش داده است اما تاثیرات آسیب پذیری هم نیز داشته است.

به گزارش دهلی نو، طی هشداری از سوی Avast، هزاران خانه هوشمند و کسب و کار در هندوستان در معرض خطر نشت اطلاعات به دلیل نقص در کانفیگ پروتکل های مورد استفاده در اتصالات خانه های هوشمند با hub ها هستند.

عموما کاربران با بی‌توجهی از تنظیمات این وسایل عبور می‌کنند و تنها با راه اندازی وسیله‌ی مورد نظر خود، از سایر مباحث چشم پوشی می‌کنند.

محققان بیش از ۴۹،۰۰۰ سرویس پیام رسان پیام تله متری (MQTT) را در اینترنت کشف کردند که به دلیل تنظیمات غلط در دسترس هستند.

این مقدار شامل ۳۲۰۰۰ سرویس دهنده (که ۵۹۵ تا از آنان در هند قرار دارد) بدون پسورد می باشد که این سرورها را در خطر نشت اطلاعات قرار می دهد.

محقق امنیتی Avast، آقای Martin Hron بیان نمود که "به طور وحشتناکی دسترسی و کنترل خانه های هوشمند مردم ساده می باشد. زیرا هنوز از دورانی که امنیت بحث اصلی دنیای تکنولوژی نبوده است پروتکل های ضعیفی وجود دارد. نیاز است تا مشتریان در خصوص اهمیت امنیت اتصال به وسایلی که بخش های مختلفی از خانه شان را کنترل می کند آگاه باشند و به درستی تنظیمات آن را اعمال کنند."

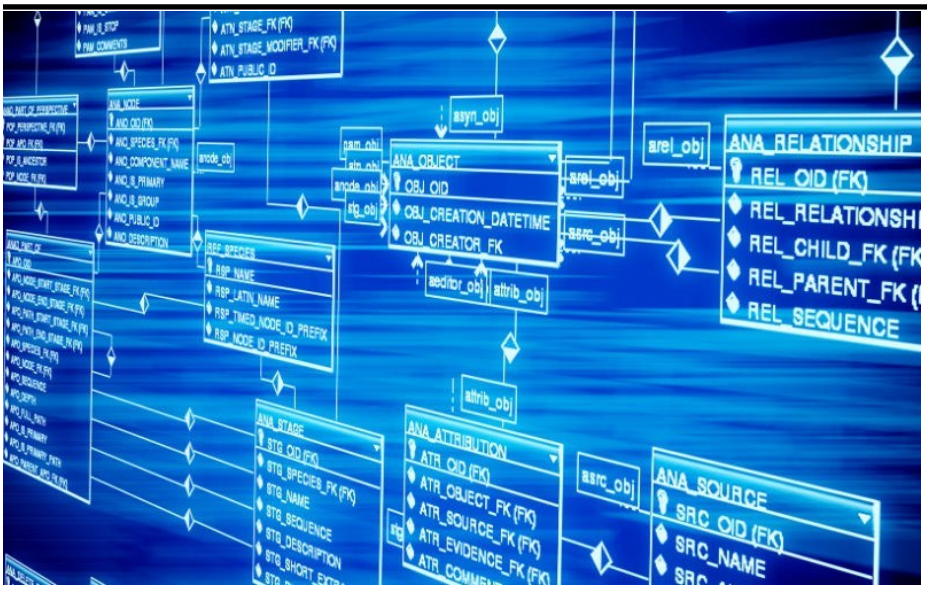
در هنگام راه اندازی پروتکل MQTT، کاربران یک سرویس دهنده را راه اندازی می کنند. در این موارد، عموما سرویس دهنده یک کامپیوتر شخصی ویا یک mini computer- همانند Raspberry Pi است که وسایل می توانند به آن متصل و ارتباط برقرار کنند.

خلافکاران سایبری می توانند دسترسی کامل به خانه ها پیدا کنند و در زمانی که صاحب خانه در خانه حضور دارد، سیستم صوتی و تصویری را آلوده نمایند و با استفاده از این سیستم ها بتوانند باز بودن ویا بسته بودن درب ها را بررسی نمایند.

در این حالت مهاجمان سایبری می توانند محل زندگی کاربر را ردگیری کنند و اطلاعات شخصی بسیار حساسی را استخراج نمایند.

گردآورنده: محمد مرتضوی

کشف آسیب پذیری روز صفر توسط تیم Trend Micro در موتور Jet مدیریت پایگاه داده‌ای مایکروسافت.



یک آسیب پذیری که قابلیت اجرای کد از راه دور را به مهاجمان می‌دهد در موتور پایگاه داده‌ای Jet مایکروسافت توسط تیم Trend Micro به تازگی کشف گردید. این باگ که در تمامی نسخه‌های ویندوز حتی windows server موجود است از زمان طراحی و پیاده سازی آن، همچنان مرتفع نگردیده است.

لذا تمامی کاربران شرکت مایکروسافت را تحت الشعاع خود قرار می‌دهد.

شرکت Trend Micro یک بازه‌ی زمانی محدود را پس از اطلاع رسانی به سازندگان برای رفع این موارد تعیین کرده است. این گروه ۱۲۰ روز زمان را تا قبل از اطلاع رسانی عمومی برای حل این آسیب پذیری تعیین کرده است. تا کنون مایکروسافت از این بازه‌ی زمانی عبور کرده است.

این آسیب پذیری یک نقص خارج از محدوده (OOB) می‌باشد که بازگشایی یک منبع Jet با عنصر OLEDB مایکروسافت علت آن است.

محققان امنیتی بیان نمودند که این نقص امنیتی در سیستم مدیریت ایندکس‌ها (index) در موتور پایگاه داده‌ای Jet قرار دارد. این نقص امنیتی می‌تواند به مهاجمان، امکان اجرای دستورات را از راه دور بدهد.

با این حال، جلوه گر این آسیب پذیری این است که برای ایجاد یک سو استفاده، تعامل کاربر با یک فایل مخرب حتما مورد نیاز می‌باشد. کد اثبات این آسیب پذیری نیز در گیت هاب به آدرس زیر قرار گرفته است.

https://github.com/thezdi/PoC/tree/master/ZDI-18-1075

این آسیب پذیری در تاریخ ۸ می به مایکروسافت گزارش شد که مایکروسافت نیز ۲ باگ مربوط به Buffer overflow در Jet را در بسته آپدیت امنیتی Microsoft Patch Tuesday update قرار داد که هنوز انتشار نیافته است. این غول نرم افزاری، این آسیب پذیری را تایید نموده است و قرار است در وصله‌ی امنیتی ماه اکتبر جای داده شود.

از آنجایی که همچنان این آسیب پذیری رفع نگردیده است شرکت Trend Micro توصیه می‌کند تا برای جلوگیری از وارد شدن لطمه به کاربران، از بازکردن فایل‌هایی که از منابع ناشناس دریافت می‌شود خود داری کنند. همچنین کاربران باید آگاه باشند تا هر فایل پایگاه داده‌ای که از موتور Jet استفاده می‌کند را با احتیاط بیشتری نسبت به قبل باز نمایند و حتما از منبع آن آگاه شوند.

گردآورنده: محمد مرتضوی

هکرها با استفاده از آسیب پذیری Peekaboo قادر به سرقت فیلم-های مربوط به دوربین‌های نظارتی شدند.

یکی از وسایلی که عموما در اتصال با اینترنت قرار دارد و می‌توان به آن از هر جایی دسترسی داشت دوربین‌های مدار بسته و نظارتی می‌باشد. از این رو این وسایل نظارتی که عموما در مکان‌های مهمی هم قرار دارند می‌توانند خطرهای جدی را ایجاد نمایند.

در این ماه خبر امکان سو استفاده از این سیستم نظارتی یکی از اخباری بود که توانست باعث ایجاد نگرانی‌های زیادی گردد.

گمان می‌رود که صدها هزار دوربین امنیتی و نظارتی که از نرم افزار Nuuo استفاده می-کنند دارای یک آسیب پذیری امنیتی هستند. محققان امنیتی شرکت Tenable این باگ را کشف کرده‌اند که شناسه‌ی CVE-2018-1149 به آن تخصیص داده شده است. این آسیب پذیری به مهاجم قابلیت اجرای کد از راه دور را در نرم افزار می‌دهد. Nuuo شرکتی است که خود را با عنوان نرم افزاری "مدیریت ویدیویی" معرفی کرده است. تجارت این شرکت مربوط به ارائه‌ی راه حل‌های نظارتی در صنایعی همچون حمل و نقل، بانکداری، دولت و مناطق مسکونی می‌باشد. Peekaboo یک آسیب پذیری Buffer Overflow است که به مهاجم امکان مشاهده و مداخله در ویدیوهای ذخیره شده‌ی نظارتی را می‌دهد. این آسیب پذیری امکان سرقت اطلاعاتی نظیر اطلاعات احراز هویت، آدرس‌های IP، پورت‌های مورد استفاده دوربین‌های نظارتی را می‌دهد.

از آنجایی که این آسیب پذیری، توانایی‌های زیادی را در اختیار مهاجم قرار می‌دهد، به مهاجمان این امکان را می‌دهد که حتی یک تصویر ثابت را به عنوان منبع دوربین‌های نظارتی قرار دهند. به علاوه این آسیب پذیری امکان از کار انداختن کامل دوربین را نیز به مهاجمان می‌دهد.

Peekaboo به طور خاص NVRMini 2 NAS و شبکه‌ی ضبط ویدیویی که همانند یک hub برای اتصال دوربین‌های نظارتی عمل می‌کنند را تحت تاثیر قرار می‌دهد. بعد از اجرای این Exploit، مهاجم دسترسی کاملی را به CMS خواهد داشت.

Gavin Millard در صحبت با ZDNet بیان نمود که شرکت‌هایی که در سراسر جهان از نرم افزار Nuuo استفاده می‌کنند شامل بانک‌ها، بیمارستان‌ها، نواحی عمومی و... می‌باشند و این سیستم نظارتی دارای کاربرد گسترده‌ای می‌باشد. تاکنون اطلاعات تکنیکالی در خصوص این آسیب پذیری ارائه نشده است. همچنان ورژن 3.9.0 این نرم افزار آسیب پذیر می‌باشد.

در حالی که روزانه وسایل جدیدی به شبکه متصل می‌شوند، راه‌های نفوذ و حمله نیز افزایش پیدا می‌کند که کاربران و شرکت‌ها را در خطری جدی قرار می‌دهند. برای آسیب پذیری مطرح شده همچنان هیچ وصله‌ی نرم افزاری ارائه نشده است. اما Nuuo در حال توسعه‌ی یک راه حل برای آن می‌باشد.

nuuo
The Intelligent Surveillance Solution

گردآورنده: محمد مرتضوی

باگ مرورگر کروم به هکر ها اجازه میدهد تا اطلاعات شخصی فیسبوک و دیگر پلتفرم‌های وب را استخراج کنند!

یک اشکال جدید کروم به مهاجمین اجازه می دهد اطلاعات خصوصی را که در فیس بوک و سایر پلتفرم های وب ذخیره شده‌اند را استخراج کنند. این اشکال بر همه مرورگرها مثل Chrome که از موتور مرورگر Blink استفاده می کنند، تاثیر می گذارد. طبق StatCounter، کروم مرورگر مورد استفاده ۵۹ درصد جمعیت اینترنت است.

باگ کروم از تگ های ویدئو و صوتی HTML استفاده میکندکه در درخواست ها از یک منبع ساخته میشوند.رون ماساس محقق امنیت Imperva، اشکال تگ های ویدیویی و صوتی را وقتی کشف کرد، که با برچسب های مختلف HTML برای ارتباطات متقابل، تحقیق می کرد.

به اشتراک گذاری منبع متقابل، مکانیزمی است که از هدرهای HTTP برای آموزش مرورگرهای وب و سرورها در مورد چگونگی استفاده از منابع متقابل دامنه استفاده می کند. این روش یک راه برای چگونگی درخواست آدرس های از راه دور را زمانی که دارای حق دسترسی هستند، تعریف می کند.

باگ کروم برای استخراج اطلاعات

رون ماساس یافت که تگ های HTML نمی‌توانند که نوع محتوا ها را تصدیق کنند و یک مهاجم میتواند ویدئو یا صوت مخفی ای را تزریق کند که پست های فیسبوک را درخواست میکند

هنگامی که کاربر از صفحه وب مهاجم بازدید میکند که حاوی ویدیوهای مخفی یا برچسبهای صوتی است که از فیس بوک پست ها را درخواست می کند و با تجزیه و تحلیل درخواست اینکه کدام پست ها برای کاربر فراخوانی می شود، مهاجمان قادر به استخراج سن کاربر از شبکه اجتماعی بدون توجه به تنظیمات حریم خصوصی میشوند

رون ماساس یک تابع جاوا اسکریپت ایجاد کرد که برآورد یک اندازه منبع را به ارمغان می آورد.

مهاجم می تواند پست های فیس بوک را برای هر سن احتمالی ایجاد کند با استفاده از گزینه های محدودیت مخاطبان که مانع دیدن پست ها بر اساس سن، موقعیت، جنسیت و سایر ویژگی ها می‌شود سن کاربر را تعیین کند.

"با استفاده از چندین اسکریپت که در هر بار تست یک محدودیت متفاوت و منحصر به فرد را اجرا می کنند، بازیگر بد می تواند نسبتا سریع مقدار مناسبی از اطلاعات خصوصی مربوط به کاربر را استخراج کند. با تجارت الکترونیک و یا مهاجمان سایت SaaS حتی می توانند آدرس ایمیل ورود را استخراج کنند. "

در حال حاضر مسئله با Chrome 68 ثابت شده است و کاربران به شدت توصیه می شوند به آخرین نسخه مرورگر کروم به روز رسانی کنند. آسیب پذیری به عنوان CVE-2018-6177 ثبت شده است.

گردآورنده: امید محمدی کیا

نشت ۱۵۷ گیگ اطلاعات!

این بار پای هکرها به شرکت‌های خودروسازی باز شد و توانست حجم بالایی از اطلاعات حساس مربوط به شرکت‌های مطرح خودرو سازی در جهان را به دست آورند.

۱۵۷ گیگابایت اطلاعات حساس شرکت‌های بزرگی مثل تویوتا و فورد و تسلا به صورت آنلاین نشت پیدا کرد و در دسترس عموم قرار گرفت.

اطلاعات حساس بیش از صد تولید کننده قطعات به صورت آنلاین منتشر شد، اطلاعات منتشر شده متعلق به غول‌های تولیدی مثل تویوتا، فورد تسلا و ThyssenKrupp است.

تیم ریسک سایبری Upguard اطلاعات نشر یافته 10 سال از شماتیک خط تولید و نقشه کارخانه و تنظیمات روبوتیک و درخواست‌های VPN و ای دی‌ها و توافقات محرمانه را یافته است

این اطلاعات به این علت منتشر شده که این کارخانجات پروتکل rsync که مربوط به پشتیبان گرفتن است را توسط IP یا کاربر محدود نکرده بودند و دیتاها به صورت عمومی در دسترس بود.

تیم Upguard یافته است که اطلاعات از یک جولای 2018 نشر یافته است.

این مسئله در تاریخ 9 ژوئیه به تامین کنندگان خودرو رده 1 رسید و برطرف کردن آن تا 10 ژوئیه انجام شد.

داده‌های منتشر شده شامل اطلاعات تماس مشتری، داده‌های مشتری مانند نام، مدال‌ها ID، اعتبار VPN و... است. داده‌های کارکنان مانند اسکن گذرنامه، گواهینامه رانندگی و سایر مدارک شناسایی.

همچنین شامل داده‌های شرکتی مانند فاکتورها، قیمت ها، محدوده کار، مشتریان، پروژه‌ها و اسناد تجاری رایج است. معلوم نیست چه کسی غیر از Upguard دسترسی به پایگاه داده دارد.

زنجیره تامین به ضعیف‌ترین بخش محرمانگی داده‌های سازمانی تبدیل شده است. شرکت-هایی که بیش از یک میلیون دلار در سال در امنیت رایانه صرف می‌کنند، هنوز هم توسط یک فروشنده که داده‌های خود را مدیریت می‌کنند، در معرض خطر قرار می‌گیرند.

گردآورنده: امید محمدی کیا

آسیب پذیری روز صفر در مرورگر Tor ورژن ۷

تیم Zerodium با انتشار توییتی از آسیب پذیری روز صفر در آخرین ورژن از مرورگر Tor خبر داد. بر اساس گفته‌های Zerodium که کار آنان خرید و فروش آسیب پذیری‌های نرم افزاری است، این مرورگر دارای یک آسیب پذیری جدی می‌باشد که یک درب پشتی با قابلیت دور زدن تمامی تدابیر امنیتی مرورگر Tor است. افزونه‌ی NoScript این مرورگر برای بلاک کردن تمامی کدهای JavaScript در سطح امنیتی "ایمن" می‌باشد. اما این درب پشتی در حتی در زمان غیرفعال بودن تمامی افزونه‌ها نیز فعال است.

یک کاربر توییتر با آی دی x0rz بیان نموده است که استفاده از این آسیب پذیری بسیار ساده است. Mukul Kumar، CISO و معاون اجرایی سایبری در Cavirin بیان نمود:"این آسیب پذیری بیش از یک آسیب پذیری ساده در یک مرورگر نگران کننده است. سطح حمله بزرگ است و هکرها دارای نقاط ورودی متعددی هستند. برای حفظ موقعیت سایبری، نیاز به سخت گیری و یک رویکرد چند لایه‌ای امنیتی است که شامل مراحل مستحکم سازی اپلیکیشن‌ها و سیستم عامل، وصله‌های امنیتی و آموزش کاربران، به جز فایروال و رمزگذاری است."

Zerodium یک پلتفرم برای آسیب پذیری‌های روز صفر می‌باشد. این کمپانی آسیب پذیری‌ها را میخرد و آنان را به دولت فدرال می‌فروشد.

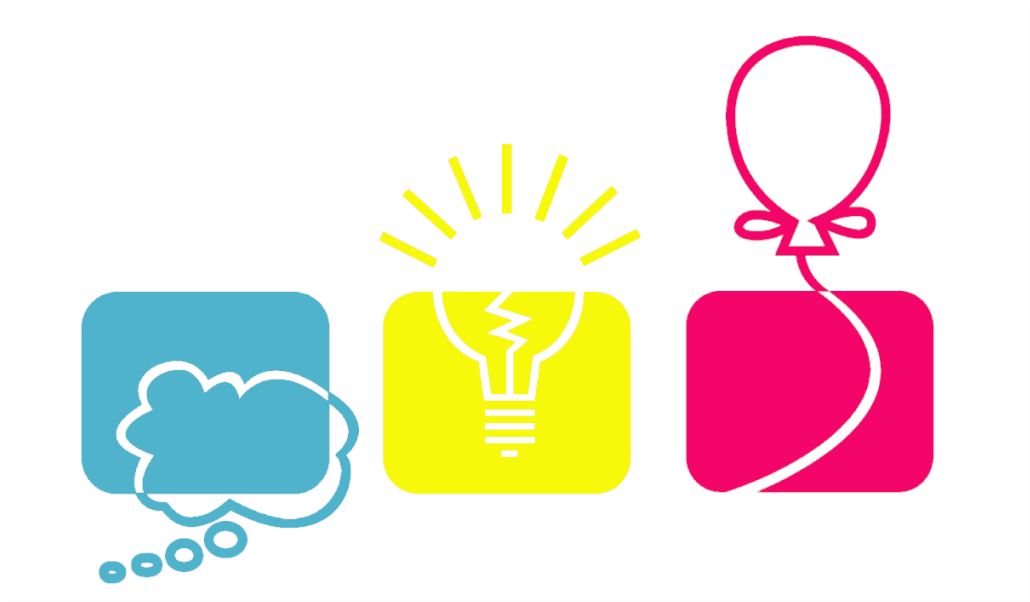
لذا توسعه دهنده‌ی NoScript آقای Giorgio Maone در توییتی اعلام نمود: "این مشکل توسط غیرفعال شدن JSON Viewer در NoScript رخ داده است. با تشکر از campuscodi برای اطلاع رسانی این آسیب پذیری روز صفر به من. ما در حال کار برروی آن هستیم".

با توجه به سخنان Morales ، سوال بزرگ در اینجا این است که آیا این آسیب پذیری توسط سازمان‌های دولتی برای دسترسی به سیستم‌هایی که به اعتقاد آن‌ها توسط افراد هدف مورد استفاده قرار می گرفته، استفاده شده است یا خیر؟

عموما از سیستم Tor در کاربری‌های قانونی استفاده نمی‌شود. معمولا در شرکت های بزرگ به عنوان یک خطر به آن نگاه می‌شود. Tor توسط مهاجمان به عنوان یک ابزار عبور از کنترل‌های امنیتی محیط برای ایجاد دسترسی از راه دور و برای فرمان و کنترل استفاده می‌شود. Tor همچنین برای عدم شناسایی فعالیت‌ها در وب استفاده می‌شود که فرد نمی خواهد نظارت یک ISP یا نهاد دولتی بر آن وجود داشته باشد. این آسیب پذیری اجازه می‌دهد که افراد دقیقا هر کاری را که انجام می‌دهند توسط شخصی دیگر مانیتور و نظارت شوند.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATOR CENTER



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.