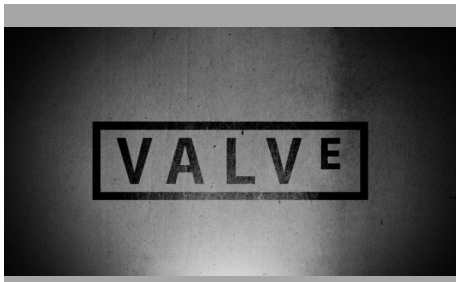
شماره هفدهم - خرداد ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



Valve نقص امنیتی که برای بیش از ۱۰ سال در سرویس دهنده Steam پنهان شده بود را رفع کرد.

اخباری این چنین، تاکید بر این حقیقت دارند که کار توسعه هرگز پایان نمی‌پذیرد و استانداردهای امنیتی مدرن می تواند موجب بروز نقص هایی در کدنویسی شود که به نظر می‌رسد بسیار قوی باشد. - صفحه ۲

- **توصیه به همه کاربران: روترهای خود را مجددا راه اندازی کنید!**

مقامات اداره تحقیقات فدرال (FBI) مصرا از کاربران خواسته اند راه اندازی مجدد روترهای خود را انجام دهند. سامانه اعلان عمومی می گوید صدها هزار دستگاه خانگی و اداری توسط "عامل سایبری خارجی" به خطر افتاده است. - صفحه ۳

داده های موقعیت مکانی در Google Home و Chromecast نشت پیدا کرده است.

داده های موقعیت مکانی در Google Home و Chromecast نشت پیدا کرده است این مشکل در حال patch شدن می باشد. خطای بسیار ناچیزدر تشخیص موقعیت مکانی با دقت چند فوت. - صفحه ۵

خرید پلتفرم مجنتو توسط شرکت ادوبی

شرکت ادوبی برای حضور در بازار تجارت الکترونیک، پلتفرم مجنتو را خریداری کرد. شرکت ادوبی توافق کرده است که شرکت تجارت الکترونیک مجنتو را به قیمت ۱.۶۸ میلیارد دلار خریداری کند تا بتواند رقیبی در صنعت تجارت الکترونیک برای Salesforce و Oracle بشود. - صفحه ۴

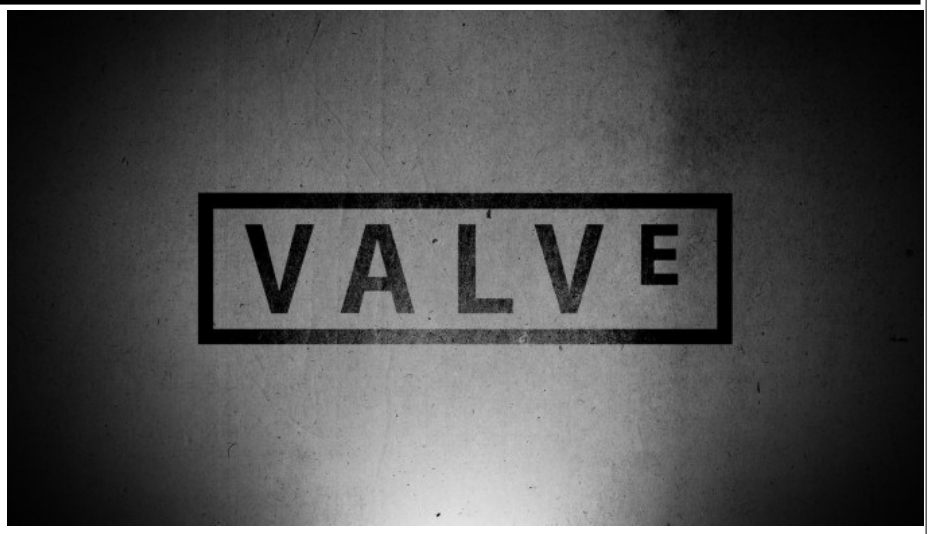
OpenVPN توضیح می دهد که کارکنان چقدر در حفظ امنیت شرکت ها بد هستند

ایجاد یک شرکت امن نیازمند کمک همه کارکنان و کاربران نهایی است. آگاهی و هوشیاری مداوم برای کمک به جلوگیری از بروز اتفاق ضروری است. پسوردهای ضعیف، استفاده مجدد از پسوردها و کلیک بر روی لینک‌های مشکوک همچنان در میان همه جوامع به عنوان مشکل باقی مانده است. - صفحه ۶

- **بدافزار VPNFilter بیش تر از تصور اولیه بر روی دستگاه‌های بیش‌تری تأثیر می‌گذارد.**

حتماً VPNFilter، بدافزار روتر چند طبقه که ماه گذشته کشف شد، را به یاد دارید. محققان سیسکو اعلام کرده‌اند که بیش از ۵۰،۰۰۰ دستگاه در بیش از ۵۰ کشور به این بدافزار آلوده شده‌اند و در پی آن FBI به کاربران پیشنهاد داده است که روترهای خود را مجدد راه‌اندازی کنند. به نظر می‌رسد که VPNFilter حتی بدتر از آن است که تصور می‌شد. - صفحه ۷

Valve نقص امنیتی که برای بیش از ۱۰ سال در سرویس دهنده Steam پنهان شده بود را رفع کرد.



اخباری این چنین، تاکید بر این حقیقت دارند که کار توسعه هرگز پایان نمی‌پذیرد و استانداردهای امنیتی مدرن می تواند موجب بروز نقص هایی در کدنویسی شود که به نظر می‌رسد بسیار قوی باشد.

Valve اخیرا یک نقص امنیتی در client Steam خود که حداقل برای دهه گذشته پنهان بوده را رفع کرده است. تا ژوئیه گذشته،کد دلخواه میتوانست از راه دور توسط فردی که این باگ را کشف کرده ، اجرا شود.

محقق امنیتی با نام Tom Court به همراه همکاران خود این نقص امنیتی را در تاریخ ۲۰ فوریه ۲۰۱۸ به Valve گزارش داد. در کمتر از هشت ساعت، یک پچ برای مشتری ها فرستاده شد. نسخه بدون نقص رسمی در اواخر ماه مارس، به client Steam رسید.

آسیب پذیری، در هسته، در یک منطقه از کد که دیتاگرام را از چندین بسته UDP دریافتی، مجددا پردازش می کند، قرار داشت که ناشی از عدم وجود یک بررسی ساده برای اطمینان از جدا شدن اولین بسته دیتاگرام است. طول بسته مشخص شده کمتر یا برابر طول کل دیتاگرام بود. Court آن را به عنوان یک اشکال اساسی توصیف کرد. احتمالا یک نظارت ساده با توجه به بررسی در همه بسته‌های بعدی وجود داشت این واقعیت که چنین اشکال ساده‌ای با چنین عواقب جدی این همه سال در چنین چارچوب مشهوری وجود داشته است، باید به عنوان یک درس برای توسعه دهندگان به کار گرفته شود تا به طور دوره‌ای کدهای قدیمی و سیستم‌ها را برای اطمینان از مطابقت با استانداردهای امنیتی مدرن بررسی کنند.

گردآورنده: حسین علیمرادی

توصیه به همه کاربران: روترهای خود را مجددا راه اندازی کنید!

حدود ۵۰۰۰۰۰ دستگاه در ۵۴ کشور تحت تاثیر قرار گرفته اند.

مقامات اداره تحقیقات فدرال (FBI) مصرا از کاربران خواسته اند راه اندازی مجدد روترهای خود را انجام دهند. سامانه اعلان عمومی می گوید صدها هزار دستگاه خانگی و اداری توسط "عامل سایبری خارجی" به خطر افتاده است. حمله سایبری روترها از چندین تولید کننده مختلف هدف گیری می شود و دست کم یک برند NAS نیز آسیب پذیر است. مهاجمان از نرم افزارهای مخرب VPNFilter برای آلوده کردن دستگاه استفاده می کنند. این نرم افزار قابلیت های متنوعی از جمله جمع آوری داده ها، خاموش کردن از راه دور و اقدامات تحلیل و تشخیص را دارد. این هشدار می گوید: "اندازه و محدوده زیرساخت های تحت تاثیر، قابل توجه است. حامل آلودگی اولیه این بدافزار در حال حاضر ناشناخته است." راه اندازی مجدد می تواند در شناسایی سیستم های آلوده کمک کند. همچنین به کاربران توصیه میکند تنظیمات مدیریت از راه دور را غیرفعال کنند، رمزگذاری را فعال کنند، رمز عبور قوی ایجاد کنند و سیستم عامل دستگاه را به روزرسانی کنند.

بیش از یک ماه پیش که چندین سازمان آمریکایی و انگلیس از جمله FBI هشدار دادند که هکرهای روسی به روترها در سراسر جهان آسیب زده، آمد. ظاهرا این حملات حداقل یک سال قبل از اینکه کشف شود رخ داده است. این هشدار، "عاملان خارجی" را در این حمله اخیر شناسایی نکرده است، بنابراین معلوم نیست آیا این وقایع مربوط هستند یا خیر. با این حال، توجه داشته باشید که راه اندازی مجدد روتر یا NAS شما به این معنا نیست که بدافزار از بین رفته باشد. طبق گفته Symantec، "بدافزار، که به نام VPNFilter شناخته می شود، بر خلاف اکثر تهدیدات دیگر IoT است؛ زیرا حتی می تواند پس از راه اندازی مجدد، همچنان قادر به حفظ حضور مداوم در یک دستگاه آلوده باشد."

با این حال، این بدان معنا نیست که هیچ چیز در چرخه قدرت دستگاه وجود ندارد. راه اندازی مجدد "Stage 2" و "Stage 3" بدافزار را به صورت موقت حذف می کند. اینها اجزایی هستند که قابلیت های مخرب دارند. این اجزاء هنوز هم می توانند با استفاده از مرحله ۱ دوباره نصب شوند، اما به نظر می رسد که این یک فرآیند دستی است.

Symantec توصیه می کند که یک تنظیم مجدد اساسی برای بازگرداندن به تنظیمات کارخانه انجام شود. این بدافزار را پاک می کند، اما تمامی تنظیمات پیکربندی شما را به طور پیش فرض مجددا تنظیم میکند. اگر به تمام جزئیات فنی علاقه مند هستید، Symantec دارای شرح کاملی از VPNFilter است که شامل تمام دستگاه های معروف شناخته شده است. QNAP همچنین مشاوره ای را برای نشان دادن دستورالعمل های گام به گام در مورد اینکه چه کاری انجام دهید اگر یک NNN QNAP آلوده داشته باشید، دارد.

گردآورنده: حسین علیمرادی

خرید پلت‌فرم مجنتو توسط شرکت ادوبی

شرکت ادوبی برای حضور در بازار تجارت الکترونیک، پلت‌فرم مجنتو را خریداری کرد. شرکت ادوبی توافق کرده است که شرکت تجارت الکترونیک مجنتو را به قیمت ۱.۶۸ میلیارد دلار خریداری کند تا بتواند رقیبی در صنعت تجارت الکترونیک برای Salesforce و Oracle بشود.

شرکت ادوبی در بیانیه‌ای اعلام کرد که سومین شرکت بزرگ خود برای ایجاد یک سیستم پایدار برای طراحی آگهی‌های دیجیتال، ایجاد وب سایت‌های تجارت الکترونیک، سایر تجربه‌های آنلاین مرتبط با مشتری و انجام معاملات را خریداری کرده است.

پلت‌فرم مجنتو برای ساخت و اجرای فروشگاه‌های آنلاین، خرید آنلاین و ترابری استفاده می‌شود. هم‌چنین به تجار کمک می کند تا به فروش محصولات خود از طریق تبلیغات در رسانه‌های اجتماعی بپردازند و از این نظر با Shopify رقابت می‌کند. شرکت مجنتو بیش از ۱۵۵ میلیارد دلار حجم ناخالص کالا را در جهان پشتیبانی می‌کند و از مشتریان آن می‌توان به شرکت‌های Canon و Rosetta Stone اشاره کرد. شرکت EBayمالک مجنتو تا سال ۲۰۱۵ بوده است و از آن به بعد، شرکت سهامی خاص Permira Holdings LLP از آن پشتیبانی می‌کند.

ادوبی به دنبال تنوع در محصولات رسانه‌ای دیجیتال است که می‌توان آن را یکی از بزرگ‌ترین شرکت‌های نرم‌افزاری در این حوزه در جهان دانست. این معامله کمی کم‌تر از خرید Adobe Omniture در سال ۲۰۰۹ است که این شرکت را یک بازیکن بزرگ در تبلیغات دیجیتال ساخته است. خرید مجنتو شرکت‌های تجارت بر بستر ابری مانند Salesforce، Oracle و SAP SE را تبدیل به رقیب ادوبی کرده است. این خرید به عنوان بخشی از کسب و کار ادوبی به نام تجربه ابری درآمد کم‌تری را تولید می‌کند و نسبت به نرم‌افزارهای خلاقی مانند فتوشاپ رشد کم‌تر و آرام‌تری دارد. سهام شرکت ادوبی پس از این خرید در معاملات گسترده یک درصد افزایش یافت. انتظار می‌رود قرارداد برای خرید مجنتو در سه ماهه سوم سال مالی ادوبی و تا زمان تصویب قانونی پایان یابد. ادوبی با این خرید، دسترسی به بازار متوسط و مشتریان بزرگ شرکت مجنتو را به دست می‌آورد و در فروشگاه‌های فیزیکی و معاملات آنلاین جای پای محکمی ایجاد می‌کند.

مدیر اجرایی شرکت مجنتو اعلام کرد که این فروش، پیشرفت تجارت شرکت را تسریع می‌کند و دیدگاه مشترک بین دو شرکت را به عنوان شرکای تجاری منعکس می‌کند. سهام یکی از رقبای اصلی مجنتو یعنی Shopify پس از اعلام این خرید ۵.۵ درصد کاهش یافت.

گردآورنده: امین زمانی

داده های موقعیت مکانی در Google Home و Chromecast نشت پیدا کرده است.

داده های موقعیت مکانی در Google Home و Chromecast نشت پیدا کرده است این مشکل در حال patch شدن می باشد. خطای بسیار ناچیز در تشخیص موقعیت مکانی با دقت چند فوت.

چرا این موضوع مهم است: برنامه های کاربردی که با این تجهیزات سرو کار دارند ممکن است مورد سوء استفاده هایی مانند اخاذی ، کمپین های تحریک آمیز و تبلیغات هدفمند قرار گیرد (به عنوان مثال، یک تبلیغ کننده می تواند تعیین کند که آیا کاربر در محل کار یا خانه است یا خیر، و به تبع آن تبلیغات مختلفی ارائه دهد).

ضعف احراز هویت بر روی دستگاه های Google Home و Chromecast که اخیرا کشف شده است می تواند به طور مؤثر به یک مهاجم در مشخص کردن موقعیت مکانی کمک کند.

کریگ یانگ، پژوهشگر Tripwire، در ایجاد یک تمرین آزمایشگاهی برای نشان دادن اینکه چگونه یک وبسایت می تواند شناسایی و کنترل صفحه یا بلندگو در یک شبکه محلی را کنترل کند به این ضعف یا مشکل برخورد کرد.

به نظر میرسد که اگر چه برنامه خانگی - که به کاربران امکان میدهد Google Home و Chromecast را پیکربندی کند - اکثر اقدامات را با استفاده از ابر Google انجام می‌دهد، برخی از وظایف با استفاده از سرور HTTP محلی انجام میشود .دستورات برای انجام دادن کارهایی مانند تنظیم نام دستگاه و اتصال Wi-Fi به طور مستقیم به دستگاه بدون هر نوع احراز هویت قابل تنظیم می باشد.

او اشاره می کند که تفاوت بین این روش و روش اصلی تشخیص موقعیت مکانی با استفاده از IP دقت آن است .دریک آزمایش،بااستفاده از آدرس IP برای تشخیص موقعیت مکانی دو مایل ، اما یانگ با اجرای نسخه ی نمایشی حمله، حدود ۱۰ متر از دستگاه فاصله داشته است.

یانگ گفته است که این حمله در ویندوز، macOS و لینوکس با استفاده از Chrome یا Firefox جواب داده است.

یانگ برای اولین بار در ماه مه، جهت اطلاع رسانی در مورد آسیب پذیری فوق الذکر با گوگل تماس گرفت ، اما تنها با پاسخ Status: Will not Fix (Forecast Behavior) به مشکل مطرح شده در گزارش روبروگردید. زمانی که Krebs درمشکل امنیتی بوجود آمده ورود پیدا کرد، گوگل آن را تغییر داد.

Krebs گزارش داده است که غول جستجو در نظر دارد تا در اواسط ماه ژوئیه یک پچ برای رسیدگی به این موضوع منتشر کند.

گردآورنده: سمیه نیاخلیلی

OpenVPN توضیح می دهد که کارکنان چقدر در حفظ امنیت شرکت ها بد هستند

ایجاد یک شرکت امن نیازمند کمک همه کارکنان و کاربران نهایی است. آگاهی و هوشیاری مداوم برای کمک به جلوگیری از بروز اتفاق ضروری است. پسوردهای ضعیف، استفاده مجدد از پسوردها و کلیک بر روی لینک‌های مشکوک هم‌چنان در میان همه جوامع به عنوان مشکل باقی مانده است.

با گذشت هر هفته، تیترهای بیشتری از هک و نقض داده‌ها مشاهده می‌گردند. در مطالعه‌ای که اخیرا توسط OpenVPN انجام شد تعدادی از عادات بد آشکار گردیده است. اگرچه که نتایج تعجب آور نیست اما به عنوان یک یادآور برای استفاده از بهترین شیوه‌ها (تجارب) برای امنیت است و شاید گاهی در نظر داشته باشید که بخش IT را گوش فرا دهید.

از میان ۵۰۰ کارمند ایالات متحده، ۲۵ درصد به استفاده از پسورد یکسان برای تقریبا همه چیز اعتراف کرده‌اند. هنگامی که یک پایگاه داده یا وب سایت هک می‌گردد، نهاده‌های مخرب سعی خواهند کرد تا از اطلاعات اعتبار کاربری بازیابی شده، با آگاهی کامل از اینکه خیلی از کاربران عادت‌های ضعیفی دارند در دیگر سایت‌ها و کسب و کارها استفاده کنند.۲۳ درصد از کارکنان بیان کردند که آن‌ها در هنگام کلیک بر روی لینک‌ها از قبل به خود زحمت نداده‌اند که سایت مقصد را چک نمایند. به عقیده من این کار بسیار نسنجیده بنظر می‌رسد. حملات مهندسی اجتماعی و فیشینگ-فعالیتی جنایی که در طی آن از طریق ارسال ایمیل و یا با داشتن یک وب سایت اطلاعات افراد مانند شماره حساب بانکی و پسورد کامپیوتر و... فاش می‌گردد و از آن‌ها جهت کسب پول و دیگر منافع استفاده می‌شود- که از لینک‌های فریبنده در ایمیل‌های بظاهر قانونی استفاده می‌کنند یک مسیر بسیار موثر برای دستیابی به ورود شده‌اند.

تایید هویت بیومتریک یک اقدام در مقابل

پسوردهای ضعیف و استفاده مجدد بسیار از پسوردها است. وجود یک ابزار نرم‌افزاری که حداقل معیارها را برای ذخیره ایمن انواع پسوردهای پیچیده در نظر دارد، نیاز بخاطر آوردن چندین عبارت را که دارای فرم خواندن راحتی نیستند را از بین می‌برد.

بیش از ۷۷ درصد کارمندان معتقدند که گزینه‌های بیومتریک برای استفاده امن هستند و ۶۲ درصد بر این تفکر هستند که این گزینه‌ها نسبت به پسوردهای قدیمی بهتر هستند.

با وجود سطح بالای اعتماد به گزینه‌های بیومتریک، تنها ۵۵ درصد از کارمندان مورد بررسی قرار گرفته، در حال استفاده از چنین تکنولوژی‌هایی شبیه اسکن اثر انگشت و تشخیص چهره هستند. لازم به ذکر است که برخی از شرکت‌ها برای احراز هویت اجازه استفاده از گزینه‌های بیومتریک را نمی‌دهند.

برای مبارزه بهتر با تهدیدات اینترنتی، کارکنان می‌بایست بخوبی آموزش داده شوند و قادر باشند تا نشانه‌های حمله‌های بالقوه را تشخیص دهند. جلسات آموزش منظم اغلب غیر جذاب هستند و برای کسانی که می‌خواهند از راه دور آموزش فن آوری ببینند بار سنگینی خواهد بود.

OpenVPN به این نتیجه رسیده است که انگیزه دادن برای گزارش نشانه‌های (پرچم‌ها) قرمز بیشتر می‌تواند کارمندان را به خود درگیر و مشغول کند و احتمال قرار گرفتن آن‌ها در عادات بد را کمتر می‌سازد.

درست همان‌طور که بعد از فعالیت‌های خاصی بهتر است دستان خود را بشویید، بهداشت سایبری مفهومی است که به دنبال بهترین شیوه‌ها برای حفظ یک محیط ایمن برای الکترونیک است. پیشگیری از آسیب‌ها نیازمند عادات خوب در همه زمان‌ها است. حتی با پروتکل‌های مناسب در یک مکان، جنگ علیه حمله‌های ناشناس هنوز دشوار است.

گردآورنده: فاطمه الهی

بدافزار VPNFilter بیش تر از تصور اولیه بر روی دستگاه‌های بیش‌تری تأثیر می‌گذارد.

حتماً VPNFilter، بدافزار روتر چند طبقه که ماه گذشته کشف شد، را به یاد دارید. محققان سیسکو اعلام کرده‌اند که بیش از ۵۰،۰۰۰ دستگاه در بیش از ۵۰ کشور به این بدافزار آلوده شده‌اند و در پی آن FBIبه کاربران پیشنهاد داده است که روترهای خود را مجدد راه‌اندازی کنند. به نظر می‌رسد که VPNFilterحتی بدتر از آن است که تصور می‌شد.

بدافزارهای مخرب که در روسیه تولید می‌شوند، می‌توانند داده‌ها را جمع‌آوری کنند، دستگاه‌های دیگر را آلوده کنند، گواهی‌نامه‌ها را سرقت کنند و حتی دستگاه را با بازنویسی یک بخش مهم از سیستم عامل، از بین ببرند. سیسکو اکنون یک ماژول جدید کشف کرده است که می‌تواند از طریق رمزنگاری SSL با متوقف‌کردن درخواست‌های وب خروجی و تبدیل آن‌ها به HTTP غیر رمزگذاری شده، کمک کند تا اطلاعات حساس به سرقت برود.

علاوه بر این، ماژول جدید می‌تواند از حملات مردی در میانه استفاده کند تا محتوای مخرب را به ترافیک وب تزریق کند. یکی دیگر از ویژگی‌های جدید کشف شده توانایی بدافزار برای آلوده کردن دستگاه‌های دیگر، از جمله رایانه‌های شخصی در همان شبکه محلی است.

به نظر می‌رسد روترهای بیش‌تری تحت تأثیر قرار گرفته‌اند. در ابتدا گفته می‌شد که تنها تعدادی از دستگاه‌های Linksys، MikroTik، Netgear، QNAP و TP-Link آسیب پذیر هستند اما به نظر می‌رسد مدل‌های بیش‌تری از این برندها همراه با روترهای Asus، D-Link، Huawei، Ubiquiti، Upvel و ZTE نیز در معرض خطر هستند.

شما می‌توانید لیست کامل آن‌ها در آدرس https://blog.talosintelligence.com/2018/06/vpnfilter-update.html مشاهده کنید.

در حالی که VPNFilter به طور عمده روترهایی را در اوکراین هدف قرار می‌دهد و یک انگیزه سیاسی را دنبال می‌کند، به شدت توصیه می‌شود که تمام صاحبان روترهای آسیب دیده، سیستم عامل خود را به روز کنند یا تنظیم مجدد کارخانه انجام دهند.

گردآورنده: امین زمانی

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

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.