شماره سوم - فروردین ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

نسخه‌ی جدید از بدافزار Xagent برای macOS

این بدافزار قادر به سرقت پسوردها، پشتیبان های آیفون و اسکرین شات هاست.

محققان امنیت در شرکت نرم افزاری آنتی ویروس "بایت دیفندر"، نسخه جدیدی از بدافزار Xagent که macOS را مورد هدف قرار می دهد، شناسایی کردند. این بدافزار می تواند به عنوان یک تروجان و بر اساس اهداف حمله سفارشی شود. محققان شباهت هایی را در کدهایی که با نسخه هایی از بدافزارهای APT28 وجود دارد، دنبال کرده اند که گروه هک در سال گذشته، به هک کردن کمیته ملی دموکراتیک ایالات متحده آمریکا متهم شد.

شرکت بایت دیفندر، به طور کامل مطمئن نیست که چگونه نسخه مک از Xagent توزیع شد ،اما می گوید از طریق یک دانلودر بدافزار شناخته شده ی macOS که Komplex نامیده می شود، در سیستم ثبت می شود. وقتی این دانلودر نصب شد، تروجان حضور دیباگر را بررسی می کند. اگر چیزی را شناسایی کرد، به منظور جلوگیری از اجراء، خود برنامه را خاتمه می دهد. در غیر اینصورت، منتظر اتصال اینترنتی می ماند تا با سرویس C&C ارتباط برقرار کند.

ظرفیت بارگذاری Xagent، شامل مدول هایی می شود که قادر به جستجوی پیکربندی سیستم مک، بارگیری فرآیندهای در حال اجراء و کدهای اجرایی است. این قابلیت ها شامل رمزهای ورود، خواندن فایل ها، عکس برداری از صفحه نمایش و سرقت پشتیبان های iOS که در واسطه مک ذخیره شده است.

شرکت بایت دیفندر خاطر نشان می سازد که سرمایه گذاری اش درباره Xagent در حال حاضر ادامه دارد. کاربران توصیه می شوند از دانلود هرچیزی که از مک اپ استور نیست، اجتناب نمایند؛ یا اینکه به خوبی توسعه دهنده را بشناسند.

گردآورنده: حسین علیمرادی

آسیب‌پذیری امنیتی ماشین "شوینده-ضدعفونی" کننده‌ی پزشکی هوشمند

دستگاه‌های دارای اینترنت اشیاء (Internet-of-Things)، همه‌ی صنایع را به سمت صنایع کامپیوتری سوق می‌دهند و موجب می‌شوند که مصرف‌کنندگان تصور کنند زندگی آن‌ها با استفاده از دستگاه های هوشمند بسیار راحت‌تر خواهد شد.

قطعاً، برخی دلایل خوب برای وصل بودن بعضی از دستگاه‌ها به اینترنت وجود دارد. به طور مثال، روشن کردن A\C از راه دور چند دقیقه قبل از رسیدن به خانه به جای اینکه آن را در کل روز در حالی که روشن است رها کنیم.

اما آیا لازم است که همه چیز به اینترنت متصل باشند؟

قطعاً نه. یک مثال آخرین گزارش مشکلی است که در مورد یک دستگاه شوینده و ضدعفونی‌کننده هوشمند(تولید شده توسط شرکت آلمانی (Miele، منتشر شده است.

دستگاه Miele Professional PG 8528، که در موسسات درمانی برای تمیز کردن و ضدعفونی کردن آزمایشگاه ها و ابزارهای جراحی استفاده می شد، به یک آسیب‌پذیری پیمایش دایرکتوری وب سرور (Web Server Directory Traversal vulnerability) دچار است.

Jens Regel از شرکت مشاوره‌ای آلمانی شیندلر اند ولف نقصی (CVE-2017-7240) را پیدا کرده است که اجازه می دهد یک مهاجمِ از راه دورِ بتواند به جای افرادی که از طرف سرور مجاز شناخته می‌شوند به دایرکتوری دسترسی داشته باشند.

پس از یک بار دسترسی، مهاجم می‌تواند که اطلاعات حساسی که در سرور ذخیره شده‌اند را به دست آورده و حتی کد مخرب خودش را وارد کرده، از سرور بخواهد که آن را اجرا کند.

Regel توضیح داد: وب سرورِ مربوطه PST10 WebServer معمولا به پورت ۸۰ گوش می‌کند و در معرض حمله ی پیمایش دایرکتوری (Directory Traversal attack) است. همچنین یک مهاجم ممکن است از این موضوع برای دسترسی به اطلاعات حساس برای استفاده در حملات پس از آن سوءاستفاده کند«

Regel همچنین اثبات مفهوم (PoC) کد مخرب برای این آسیب‌پذیری را منتشر کرد، که این به این معناست که حالا هکر می‌تواند از این آسیب‌پذیری قبل از اینکه یک پچ (patch) عرضه شود، سوءاستفاده کند.

اجرا کردن این اکسپلویت PoC برای همگان راحت است:

GET /../../../../../../../../../../../etc/shadow HTTP/1.1 to whatever IP the dishwasher has on the LAN.

اگرچه معلوم نیست که Miele از چه کتابخانه هایی برای ساختن وب سرور استفاده کرده است، با توجه به سخنان Regel، او قادر است که به فایل سایه ی سیستم تعبیه‌شده embedded system's shadow file و با افزایش سطح دسترسی، به هر فایلی درخواست دهد.

کارشناسان امنیتی، این آسیب‌پذیری را به صورت خصوصی برای Miele در نوامبر ۲۰۱۶ فاش کردند اما برای بیش از سه ماه پاسخی از سمت او دریافت نکردند. بنابراین، اینکه آیا پچی برای این آسب‌پذیری وجود دارد یا خیر و یا زمان مورد انتظار برای آن نامعلوم است.

بنابراین، بهترین انتخاب برای اینکه خود را ایمن نگه دارید، قطع کردن اتصال دستگاه از اینترنت تا زمانی است که پچ آن منتشر شود.

گردآورنده: حسین علمیرادی

انتشار آپدیت سوییچ های D-Link

D-Link آپدیت سخت افزار مربوط به سوییچ های stackable managed را برای پوشش دادن آسیب پذیرهای جدی که منجر به نفوذ از راه دور به ابزار میشد را منتشر کرده است.

محققان امنیتی آدیتیا کی سود و ورنگ امین دریافتند سوییچ های DGS-1510 شرکت D-link که برای بنگاه های اقتصادی کوچک و متوسط توصیه می شوند دارای طراحی احراز هویت ناامن هستند. به گفته این محققان، یک مهاجم از راه دور می تواند با بهره گیری از عیوب دور زدن احراز هویت دستوراتی را روی سوییچ اجرا کند و پیکربندی و اطلاعات دیگری را استخراج کند.

محققان یک روند اثبات ایده را در اختیار securityweek قرار دادند که نشان میدهد چطور یک مهاجم احراز هویت نشده، می تواند اطلاعات کاربر که شامل نام کاربری و رمزعبور می شود را به دست آورد و یا یک کاربری با دسترسی مدیر اضافه کند. این روند اثبات ایده در زمان دیگری در دسترس عموم قرار خواهد گرفت.

امین و همکارانش بیان کردند که چندین سیستم روی شبکه شناسایی کرده اند اما نتوانسته اند به طور دقیق مشخص کنند به چه تعداد وسیله تحت وب از راه دور نفوذ شده است.

D-link در پاسخ توضیح داد که این آسیب پذیری ها تحت عنوان فرمان دور زدن احراز هویت نشده و افشاگری اطلاعات احراز هویت نشده طبقه‌بندی می‌شوند. این عیوب در مدل های

- DGS-1510-28XMP
- DGS-1510-28X
- DGS-1510-52X
- DGS-1510-52
- DGS-1510-28P
- DGS-1510-28
- DGS-1510-20

نام برده که سخت افزار با نسخه قبل هست ۱.۳۱. B003 می باشد

به روز رسانی سخت افزاری که حفره های امنیتی را پوشش میدهد هم اکنون در وضعیت بتا می باشد ودر صورتی که تست های کیفیت بلند مدت را با موفقیت پشت سر بگذارد در دسترس عموم قرار خواهد گرفت. این مشکلات در ژانویه به D-link گزارش شد و در ۲۱ فوریه در دسترس عموم قرار گرفت. حفره های امنیتی جدی در محصولات D-link یافت شده است که شامل دوربین ها، نقاط دسترسی، مودم ها، روترها و محصولات ذخیره سازی اطلاعات و سایر محصولات متصل خانگی می شود. در اوایل ژانویه کمیسیون تجارت فدرال آمریکا شکایتی علیه این تامین کننده تایوانی تجهیزات شبکه ثبت کرد که در آن این شرکت را متهم به ادعاهای نادرست در خصوص امنیت محصولاتش نمود. D-link تصمیم دارد به جنگ آنچه اتهامات بی پایه و غیر واقعی خوانده برود.

گردآورنده: حسین علیمرادی

یک گروه جاسوسی روسی بنام APT29 با تکنیک"دامنه نما" توانست عبور و مرورهای غیرعادی را برای سازمان‌های هدف سخت‌تر کند

دامنه نما روش بازرسی اطلاعات به شکل جانبی ست که شامل تغییر قیافه دادن عبور و مرور میشود تا بنظر بیاید به میزبانی که بازرس اطلاعات به آن مجوز داده است میرود، مثل گوگل، آمازون یا کلودفلر-cloudflare شرکت سیستم های Open Whisper اخیرا روشی برای کمک به کاربران نرم‌افزار سیگنال در مصر و امارات برای عبور از سانسور دولتی، انجام داده است.

براساس گزارش فایر آی؛ این روش حداقل ۲سال است بوسیله ی عامل تهدیدآمیز APT29 استفاده میشود، که بنامهای دوک ها، خرس راحت و دوک راحت نیز شناخته میشود. این گروه بعنوان عامل پشت صحنه ی حمله ی انتخاباتی اخیر در آمریکا و لشکری که سازمانهای مشخصات بالا را در نروژ هدف قرار دادند شناخته میشود.

APT29 از شبکه تُر -Tor- برای ارتباط با ماشینهای آلوده شده استفاده کرده است، که میتوانست توسط بعضی از پدافندگرها مشکوک بحساب آید. برای تغییر قیافه دادن عبور و مرور تُر به عبور و مرور ظاهرا قانونی، جاسوسان سایبری از میک استفاده کردند، یک پلاگین از تُر که جلوقراردادن دامنه را اجرا میکند و به کاربران اجازه میدهد که عبور و مرور را با شکل درخواست بی‌ضرر HTTPS POST به گوگل، به تُر بفرستند.

در حملاتش، APT29 از PowerShell و یک فایل با پسوند bat برای نصب Tor client و پلاگینِ میک - Meek plugin- در سیستم هدف، استفاده کرد. آنها به شاهکاری نفوذ کردند که شامل خصیصه ی دسترسی کلیدهای چسبنده میشد، جایی که آنها اجراپذیر قانونی را با Windows Command Prompt (cmd.exe)جابجا کردند. چنین چیزی برای مهاجم شرایطی را فراهم میکند تا از آن برای دستورات اجرایی با امتیازات در سطح سیستم (SYSTEM-level) استفاده کنند که شامل اضافه کردن یا مدیریت حساب میشود.

محیطی که شاهکار کلیدهای چسبنده را اجرا میکند، سرویس ویندوزی را نیز بنام "بروزرسانی گوگل" بوجود می آورد برای اطمینان از راه فراری که حتی بعد از دوباره راه اندازی سیستم باقی بماند.

متیو دان وودی از فایر آی میگوید: APT29 دامنه نما را خیلی قبل تر از این شهرت گسترده، در بین خود پذیرفت. با بکارگیری یک اجرای در دسترس عموم، قادر شدند که عبور و مرور شبکه‌ای خود، بهمراه تحقیق و توسعه ی جزئی و با ابزارهایی که حمل آنها سخت است را پنهان کنند. تشخیص این فعالیت روی شبکه، نیازمند پدیداری در ارتباطات TLS و امضاهای شبکه ای موثر است.

گردآورنده: حسین علیمرادی

سیسکو نسبت به یک آسیب‌پذیری جدی Zero-day برای IOS/IOS XE که بر روی بیش از ۳۰۰ مدل از سوییچ هایش تاثیر می‌گذارد، هشدار داده است!

این شرکت در هنگام تحلیل «Vault 7» بالاترین سطح از آسیب‌پذیری را در محصول خود شناسایی کرده است. تقریبا ۸۷۶۱ سند و فایل در هفته‌ی گذشته توسط ویکی‌لیکس منتشر شد که ادعا می‌کردند به جزییات ابزار هک و تاکتیک‌های سازمان اطلاعات مرکزی (سیا) دست یافته‌اند.

این آسیب‌پذیری در پروتکل مدیریت خوشه‌ای (CMP) واقع است که Cisco IOS و نرم افزار Cisco IOS XE را پردازش می‌کند.

اکسپلویت CVE-2017-3881 می‌تواند به یک مهاجم از راه دورِ غیرمجاز اجازه دهد که سبب انجام یک ری‌بوت روی یک دستگاه قربانی شود یا اینکه از راه دور کدهای مخرب روی دستگاه اجرا کند و همه ی کنترل دستگاه را در دست بگیرد.

پروتکل CMP برای این طراحی شده است که اطلاعات مربوط به سوییچ‌های خوشه ای (switch clusters) بین اعضای خوشه‌ای که از Telnet یا SSH استفاده می کنند راعبور دهد.

این آسیب‌پذیری بر روی پیکربندی پیش‌فرض دستگاه‌های قربانی وجود دارد، حتی اگر کاربر هیچ کدام از فرمان های پیکربندی خوشه‌ای را اجرا نکند. این نقص امنیتی می‌تواند در Telnet session با هر کدام از نسخه های IPv4 یا IPv6 اکسپلویت شود.

با توجه به گفته‌ی محققان Cisco، این باگ در اتصالات Telnet با استفاده از CMP رخ می‌دهد و دو عامل باعث رخداد آن است:

پروتکل، استفاده از گزینه مخصوص Telnet در CMP را فقط برای ارتباطات داخلی و محلی بین اعضای خوشه‌ای محدود نمی‌کند؛ در عوض، پروتکل هر فرمانی روی هر اتصال Telnet به یک دستگاه قربانی را قبول و پردازش می‌کند.

پردازش غلط آپشن‌های ناقص Telnet که مخصوص CMP هستند.

محققان می‌گویند برای اکسپلویت کردنِ این آسیب‌پذیری، یک مهاجم می‌تواند "در حالی که یک Talent session در حال ایجاد است، آپشن‌های ناقص Telnet را با استفاده از یک دستگاه قربانی که برای قبول اتصالات Telnet پیکربندی شده است ارسال کند."

این اکسپولیت کردن ممکن است به مهاجم اجازه دهد که از راه دور کد مخربی را اجرا کند و کنترل کامل دستگاه را به دست گیرد یا سبب ری لود شدنِ دستگاه آسیب‌دیده شود.

Telnet را روی مدل‌های آسیب پذیر غیرفعال کنید – پچ هنوز در دسترس نیست

این آسیب پذیری روی۲۶۴ Catalyst switches، ۵۱ industrial Ethernet switches و ۳ دستگاه دیگر که شامل موارد زیر است، تاثیر می‌گذارد:

- Catalyst switches
- Embedded Service 2020 switches
- Enhanced Layer 2/3 EtherSwitch Service Module
- ME 4924-10GE switch، IE Industrial Ethernet switches
- SM-X RF Gateway 10، Layer 2/3 EtherSwitch Service Module
- Gigabit Ethernet Switch Module (CGESM) برای HP و

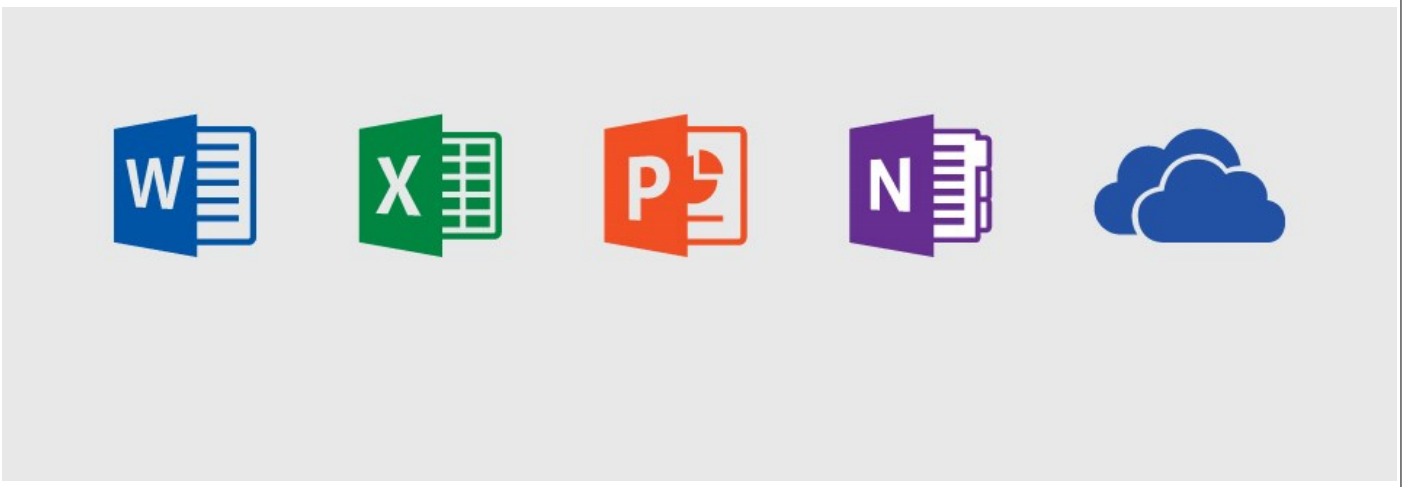
در حال حاضر، این آسیب‌پذیری پچ نشده است و تا زمانی که پچ‌های آن در دسترس قرار بگیرند، Ciscoبه کاربرانش پیشنهاد می‌کند که اتصال Telnetبه دستگاه سوییچ را به خاطر SSH غیرفعال کنند.

راهنمای امنیتی شرکت درباره‌ی انجام هیچ اکسپلویتی با استفاده از این نقص صحبت نمی‌کند اما اگر موردی وجود داشته باشد،به نظر می‌رسد، ده‌ها هزار، اگر صدها هزار نباشند، از دستگاه‌های نصب شده در سرتاسر جهان در معرض یک ریسک بزرگ برای یک مدت نامعلوم قرار خواهند داشت.

Cisco ابزار بررسی کننده‌ی نرم‌افزار IOS را بلافاصله پس از اینکه پچ‌ها بیرون بیایند، آپدیت خواهد کرد.

گردآورنده: حسین علیمرادی

هکرها در حال استفاده از یک نقص امنیتی Zero-day در اسناد Microsoft Word برای نفوذ هستند!



محققان امنیتی یک حمله روز صفر جدید کشف کردند که به طور پنهانی از طریق Microsoft word قادر به نصب بد افزار برروی کامپیوترهایی که به طور کامل دارای تمامی وصله های نرم افزاری می باشند.

شرکت های McAfee و FireEye مطلبی را در بلاگ خود مطلبی مبنی بر کشف یک حمله قرار دادند که این حمله با یک فایل مخرب که به یک ایمیل پیوست شده است شروع می شود. در این مورد، سند word گفته شده شامل یک exploit جاسازی شده می باشد. زمانی که این سند باز می شود، یک درخواست HTTP به آدرسی که تحت کنترل حمله کننده است فرستاده می شود تا باقی فایل های برنامه های مخرب (HTA) که در قالب فرمت RTF هستند دانلود شود.

فایل hta. به صورت خودکار اجرا می شود و به حمله کننده اجازه می دهد تا از اجرای کدها بهره برداری کاملی داشته باشد و باقی فایل های مورد نیاز را از خانواده های بدافزاری شناخته شده مختلف دانلود کند.

ذات این حمله به گونه ای است که می تواند اکثر طراحی های مبنی بر کاهش حافظه ی مایکروسافت را دور بزند. این حمله برخلاف باقی exploit های word برروی تمامی نسخه های سیستم عامل ویندوز، حتی ویندوز ۱۰ قابل اجرا می باشد. این حمله نیازی به فعال بودن Macro ها در word ندارد. این حمله باعث می شود تا یک سند word جعلی به کاربر نمایش داده شود و فعالیت ها به صورت پنهانی برروی کامپیوتر قربانی انجام گیرد.

شرکت های McAfee و FireEye اعلام کردند که این آسیب پذیری مربوط به بخش ارتباط و تعبیه ی اشیا (OLE) در ویندوز می باشد که ابزاری برای ارتباط و پیاده تعبیه ی اسناد به سایر اشیا می باشد.

شرکت FireEye اعلام کرده که آن ها چندین هفته می باشد که در حال کار برروی این آسیب پذیری می باشند و قرار بوده که تا زمانی که مایکروسافت یک وصله نرم افزاری برای آن ارائه نکرده این امر را فاش نسازند. اما پس از اعلام این اطلاعات توسط McAfee، آنان نیز تصمیم به ارائه ی اطلاعاتی کردند که به آن دست یافته اند.

مایکروسافت اعلام نموده که اصلاح این مورد به صورت بخشی از آپدیت های نرم افزاری ماهانه در دسترس قرار خواهد گرفت. اما همیشه به خاطر داشته باشید که در خصوص فایل های مشکوکی که توسط ایمیل برای شما می آیند، حتی اگر فرستنده آن را می شناسید کاملا هوشیار باشید.

گردآورنده: محمد مرتضوی

پایان راه ویندوز ویستا

ویندوز ویستا، یکی از منفورترین ورژن های سیستم عامل مایکروسافت، برای همیشه به خاطره ها پیوست. طبق گزارشات گذشته، ۱۱ آپریل روز پایان زندگی این سیستم عامل قدیمی معرفی شده بود. از این پس هیچ آپدیت امنیتی و غیر امنیتی، پشتیبانی رایگان و یا پولی از سوی مایکروسافت برای این سیستم عامل ارائه نخواهد شد.

ویندوز ویستا هنوز انتخاب اول ۰.۷۲ درصد از کاربران سیستم عامل ویندوز می باشد. به این معنی که در حدود ۱۰ الی ۱۱ میلیون کاربر از این سیستم عامل استفاده می کنند. در مقایسه با ویندوز اکس پی، این مقدار ۷.۴۴ درصد می باشد.

مایکروسافت اعلام کرده است به مدت ۱۰ سال از این سیستم عامل پشتیبانی شده است اما زمان آن فرا رسیده است که با توجه به شرکای سخت افزاری و نرم افزاری، منابع را برروی تکنولوژی های جدیدتر برای رسیدن به تجربیات بزرگ سرمایه گزاری کنند.

پشتیبانی اصلی از ویستا در تاریخ ۱۰ آپریل ۲۰۱۲ به پایان رسیده بود اما برای سرویس پک دو این سیستم عامل، این پشتیبانی برای مشتریان تجاری ادامه داشت.

به گفته ی برخی از کاربران، ویندوز ویستا سزاوار به دست آوردن شهرت نبود و مسائل مربوط به عملکرد آن به دلیل استفاده شدنش توسط کامپیوترهای خانگی می باشد. علاوه بر این، از روی علاقه سیستم عامل ویستا را می توان به عنوان سنگ فرش راه ویندوز ۷ دانست.

افرادی که به استفاده از ویندوز ویستا ادامه می دهند از امروز به بعد ممکن است در مقابل ریسک ها و ویروس ها آسیب پذیر باشند. همچنین با پشتیبانی نکردن ویندوز ویستا از اینترنت اکسپلورر ۹ از این پس افرادی که از این مرورگر استفاده می کنند بیشتر در مقابل خطرات تهدید می شوند. مرورگرهای دیگری مانند گوگل کروم نیز قبل تر پشتیبانی خودرا از ویندوز ویستا پایان داده بودند.

مایکروسافت اضافه کرد: همانطور که شرکت های سخت افزاری و نرم افزاری بیشتری محصولاتشان را برای نسخه نهایی سیستم عامل ویندوز بهینه می کنند، شما با برنامه های کاربردی بیشتر مواجه خواهید شد که با این ویندوز دیگر سازگاری نخواهند داشت.

خدانگهدار ویستا. حدود ۳ سال دیگر نوبت به ویندوز ۷ خواهد رسید.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

نشانی:

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

مدیر مسئول:

دکتر امید مهدی عبادتی

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

هیات علمی:

دکتر احسان ملکیان

وب سایت:

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

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد