بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و چهارم

شهریور ماه ۱۳۹۹

رفع نقص‌های امنیتی، این بار در وب سرور APACHE

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی، سهیلا مرادی**

سردبیران:

سیده مرضیه حسینی

صبا آزرمی

با همکاری

سیده آرزو حسنی

آدرس:

کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱

apa@razi.ac.ir

@APARazi

cert.razi.ac.ir

اخبار امنیتی

حمله به سایت‌های وردپرس با افزونه آسیب‌پذیر File Manager

به گزارش کارشناسان، عاملان تهدید به طور فزاینده‌ای آسیب‌پذیری اخیر در افزونه File Manager وردپرس را مورد هدف قرار داده‌اند. محققان شرکت امنیتی WordPress مشاهده کردند که تعداد حملاتی که این آسیب‌پذیری را مورد هدف قرار می‌دهند افزایش یافته است.

هکرها یک آسیب‌پذیری بحرانی اجرای کد از راه دور یا همان remote code execution را در افزونه File Manager مورد اکسپلویت قرار می‌دهند که می‌تواند توسط مهاجمان غیرمجاز برای بارگزاری اسکریپت‌ها و اجرای کد دلخواه بر روی سایت‌های وردپرسی که نسخه آسیب‌پذیر این افزونه را در حال اجرا دارند، مورد بهره‌برداری قرار گیرد. این افزونه که در حال حاضر در بیش از ۷۰۰,۰۰۰ سایت وردپرسی نصب شده است به کاربران امکان می‌دهد تا به راحتی فایل‌ها را مستقیما از وردپرس مدیریت کنند.

این آسیب‌پذیری اولین بار توسط Gonzalo Cruz از Arsys کشف و شناخته شد، به گفته این محقق عاملان تهدید از این نقص برای بارگزاری فایل‌های مخرب PHP در سایت‌های آسیب‌پذیر وردپرس استفاده می‌کنند.

آسیب‌پذیری مذکور تمام نسخه‌های بین ۶.۰ تا ۶.۸ این افزونه محبوب را تحت تاثیر قرار می‌دهد. توسعه دهندگان این افزونه با انتشار نسخه ۶.۹ آسیب‌پذیری مذکور را رفع و وصله کرده‌اند.

Cruz یافته‌های خود را با شرکت امنیتی Wordfence به اشتراک گذاشته و کد اثبات مفهومی اکسپلویت این آسیب‌پذیری را نیز به آنها ارائه داده است. این شرکت امنیتی نیز با تایید این حملات، با استفاده از WAF (Web Application Firewall) طی چند روز گذشته بیش از ۴۵۰,۰۰۰ تلاش مهاجمان برای اکسپلویت را مسدود کرده است.

با توجه به اطلاعات دریافت شده از فایروال، به نظر می‌رسد که مهاجمان ممکن است فایل‌های خالی را جستجو کنند و در صورت موفقیت می‌توانند یک فایل مخرب را درون وب‌سایت آسیب‌پذیر تزریق نمایند. از جمله فایل‌هایی که توسط مهاجمان بارگزاری شده‌اند می‌توان به hard-fork.php، hardfind.php و x.php اشاره کرد.

کارشناسان Wordfence اذعان دارند که عوامل تهدید در تلاشند تا فایل‌های PHP را با webshellsهای مخفی شده در تصاویر موجود در مسیر wp-con-tent/plugins/wp-file-manager/lib/files/ folder بارگزاری کنند.

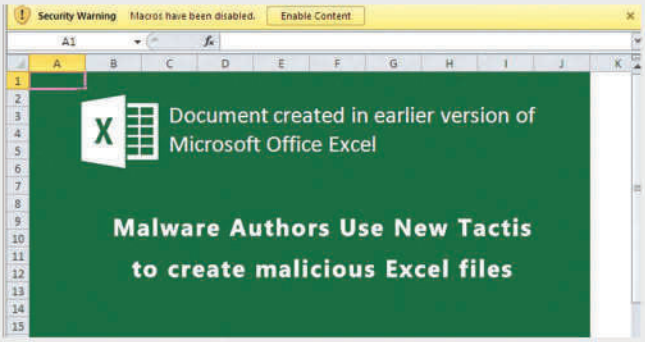
چند روز پس از رفع آسیب‌پذیری و انتشار نسخه وصله شده افزونه فوق، مهاجمان اقدام به هدف قرار دادن نسخه‌های وصله نشده کرده‌اند و تعداد حملات به 2.6 میلیون رسیده است.

به کاربران توصیه می‌شود در صورتیکه از نسخه آسیب‌پذیر افزونه File Manager استفاده می‌کنند سایت خود را به منظور شناسایی بدافزار با استفاده از یک راه‌حل امنیتی مانند Wordfence اسکن کنند و در اسرع وقت نسبت به نصب نسخه وصله شده اقدام نمایند.

منبع خبر :

Scan Link

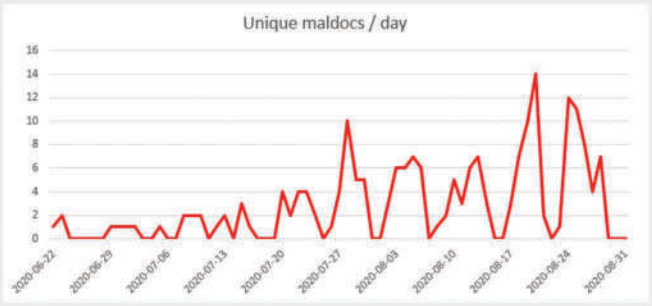
امکان دور زدن پروتکل‌های امنیتی در پی نقص نرم‌افزار محبوب Excel



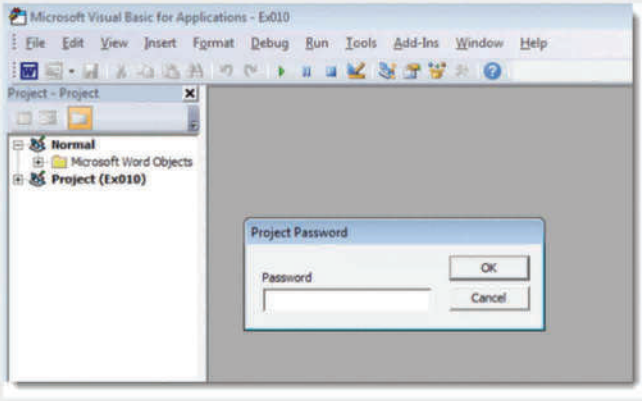
توسعه‌دهندگان بدافزارها با بکارگیری تکنیک جدیدی، این امکان را خواهند داشت تا بدون استفاده از مایکروسافت آفیس، کاربرگ‌های[1] macro-laden را در نرم‌افزار اکسل ایجاد کنند. محققان امنیتی NVISO، اسناد مخرب اکسلی را شناسایی کردند که بدافزار را از طریق VBA[2] فعال منتقل خواهد کرد.

براساس تجزیه و تحلیل‌های NVISO، مشخص شد که اسناد مخرب با استفاده از نرم افزار EPPlus در قالب OOXML[3] ایجاد می‌شوند که در واقع یک OPC[4] است که عمدتاً شامل پرونده‌های XML و برخی از پرونده‌های باینری می‌باشد.

طبق پست منتشر شده از NVISO :"هنگامی که پروژه VBA توسط EPPlus ایجاد شود، شامل کد VBA کامپایل شده نیست. EPPlus هیچ روشی برای ایجاد کد کامپایل شده ندارد و مایکروسافت مسئول ایجاد الگوریتم‌هایی برای ساخت کد کامپایل شده VBA، می‌باشد." اولین نمونه با استفاده از این روش در ۲۲ ژوئن سال ۲۰۲۰ مشاهده شد و از آن زمان بیش از ۲۰۰ سند مخرب طی ۲ ماه شناسایی شدند.



تمامی اسناد مخرب از طریق رمزعبور، از پروژه VBA محافظت کرده و باز کردن این پروژه‌ها فقط با وارد کردن رمزعبورشان امکان‌پذیر می‌باشد



هنگامی که کاربر، اسناد مخرب را باز می‌کند، پی‌لودی از سایت‌های مختلف دانلود شده که توسط عاملان بدافزار کنترل می‌شود؛ پی‌لود به عنوان یک dropper ایفای نقش کرده و موتورهای آنتی‌ویروس، بدافزار را به عنوان AgentTesla شناسایی می‌کنند.

گفتنی است که مهاجمان از حساب‌های ایمیل متعلق به شرکت‌ها، جهت ارسال ایمیل Spam استفاده می‌کنند و از طرفی نیز با بررسی فرستنده و گیرنده ایمیل، الگویی جهت شناسایی آن‌ها، وجود ندارد.

کشورهایی همچون ایالات متحده، جمهوری چک، فرانسه، آلمان و همچنین چین هدف اصلی این حملات می‌باشند و NVISO معتقد است که تکنیک ایجاد اسناد مخرب اکسل، بیشتر از این نیز مورد استفاده قرار خواهد گرفت.

منبع خبر :

Scan Link

جاسوس‌ابزار مبتنی بر پایـــــتون RAT PyVil

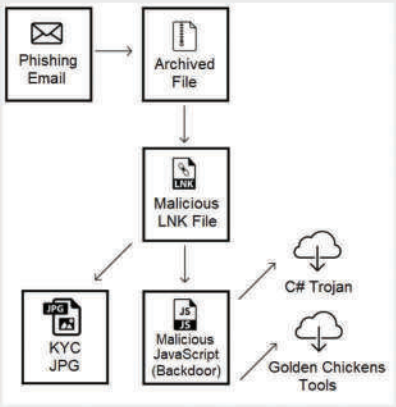
[1] worksheet
[2] VBA مخفف Visual Basic for Applications یک زبان برنامه نویسی است که در مجموعه برنامه‌های آفیس استفاده می‌شود.
[3] Office Open XML
[4] Open Packaging Conventions

اخیراً گروه Evilnum APT از ابزار مبتنی بر پایتون RAT PyVil برای جاسوسی و سرقت اطلاعات حساس استفاده می‌کند. انگیزه اصلی این گروه، جاسوسی از قربانیان و سرقت تمام رمزهای عبور VPN، اطلاعات ورود ایمیل، اسناد مختلف و کوکی‌های مرورگر است.

این اولین بار نیست که این گروه جاسوسی اقدام به چنین حملاتی می‌کند، این گروه در اوایل سال ۲۰۱۸ نیز نسبت به چنین حملاتی اقدام کرده بودند، اما این بار آنها با ایده‌ها و ترفندهای جدیدی برای سرقت اطلاعات حساس قربانیان اقدام به حملات جدید کرده‌اند.

به گفته کارشناسان، Evilnum با استفاده از عناصری که در جاوااسکریپت و C# نوشته شده‌اند، اقدام به این حملات نموده‌اند. آنها همچنین از ابزارهای مختلف- Golden Chickens ارائه دهنده سرویس‌های بدافزار- و عموما از ایمیل‌های فیشینگ برای انجام حملات خود استفاده می‌کنند.

PyVil RAT به مهاجمان این امکان را می‌دهد تا تمام داده‌ها از جمله اطلاعات ورود به سیستم را استخراج کرده و از آنها عکس بگیرند. همچنین می‌توانند از ابزارهای ثانویه جمع‌آوری اطلاعات ورود مانند LaZagne استفاده کنند، LaZagne یک اپلیکیشن اوپن‌سورس است که برای سرقت رمزهای عبور ذخیره شده بر روی یک کامپیوتر محلی استفاده می‌شود.



به گفته کارشناسان امنیت سایبری Cybereason Nocturnus این نسخه جدید PyVil با قابلیت‌های بسیاری ایجاد شده است که از جمله آنها می‌توان به موارد زیر اشاره کرد:

- کی‌لاگر[1]
- اجرای دستورات cmd
- گرفتن عکس از صفحه
- دانلود اسکریپت‌های دیگر پایتون برای قابلیت‌های بیشتر
- بارگزاری فایل‌های قابل اجرا
- باز کردن یک SSH shell
- جمع‌آوری تمام داده‌ها مانند برنامه‌های آنتی‌ویروس نصب شده، دستگاه‌های USB متصل و نسخه‌های مرورگر کروم

الگوهای حمله Evilnum

Evilnum همواره بر ایمیل‌های فیشینگ تکیه کرده است که شامل آرشیوهای ZIP در فایل‌های LNK 4 است به همین دلیل الگوهای این حمله و نسخه جدید آن با ایده‌ها و ترفندهای جدید ساخته شده است.

برنامه‌های آسیب‌پذیر استفاده شده

برنامه‌های آسیب‌پذیری که در این حمله استفاده می‌شود عبارتند از:

- DDPP.exe
- FPLAYER.exe

✓ توصیه امنیتی

کارشناسان شرکت امنیت سایبری به کاربران توصیه می‌کنند:

- مجموعه ابزارهای امنیتی خود را به طور دائم بروزرسانی کنند تا بتوانند ترفندهای حملات جدید را به راحتی شناسایی کنند.
- پیوست‌های ایمیل را از منابع ناشناس دریافت نکنند.
- داده‌ها را از وب‌سایت‌های مشکوک دانلود نکنند.

منبع خبر :

Scan Link

آسیب‌پذیری روزصفر در SANDBAX ویندوز ۱۰

اخیراً آسیب‌پذیری روز صفر شناسایی شده در ویندوز ۱۰ امکان ایجاد فایل در فولدر "system 32" را برای کاربران غیر مجاز فراهم می‌آورد. این فولدر جزء ناحیه محدود شده[2] سیستم عامل است که اطلاعات حیاتی سیستم‌عامل و نرم افزارهای نصب شده آن در این فولدر نگهداری می‌شود. این آسیب‌پذیری فقط در دستگاه‌هایی که ویژگی Hy-per-V در آن‌ها فعال است، وجود دارد که این عامل موجب کاهش تعداد دستگاه‌های هدف این حمله می‌شود. چراکه این ویژگی به صورت پیش‌فرض در نسخه‌های Pro، En-terprise و Education از ویندوز ۱۰ فعال نیست.

ویژگی است که ویندوز ۱۰ برای ایجاد ماشین مجازی مورد استفاده قرار می‌دهد. با فراهم سازی منابع سخت‌افزار کافی، Hyper-V می‌تواند ماشین‌های مجازی بزرگ با ۳۲ پردازنده و ۵۱۲ گیگ RAM را اجرا نماید. یک کاربر عادی ممکن است، هیچ‌گاه نیاز به اجرای ماشین مجازی با این مشخصات نداشته باشد؛ اما کاربران عادی ممکن است مایل باشند تا Sandbox ویندوز را اجرا نمایند که استفاده از این ویژگی به صورت خودکار Hyper-V را فعال می‌نماید.

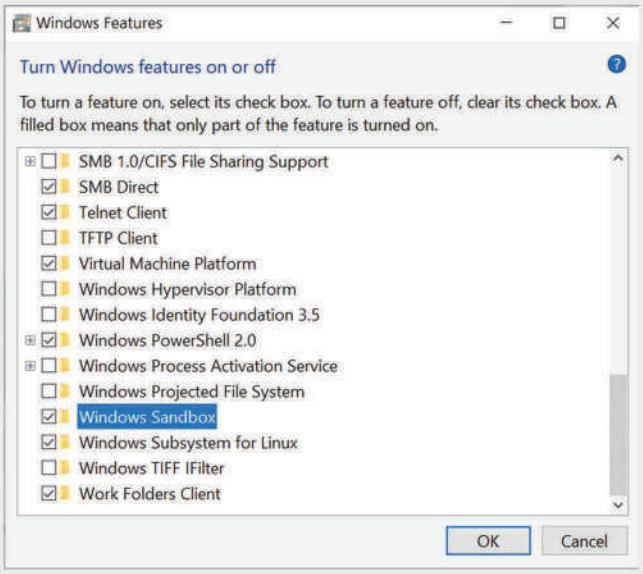
مایکروسافت در به‌روزرسانی ماه می سال ۲۰۱۹، Sandbox را در نسخه ۱۹۰۳ از ویندوز ۱۰ معرفی کرد. کاربران با فعال سازی Sandbox می‌توانند در محیط ایزوله و

---

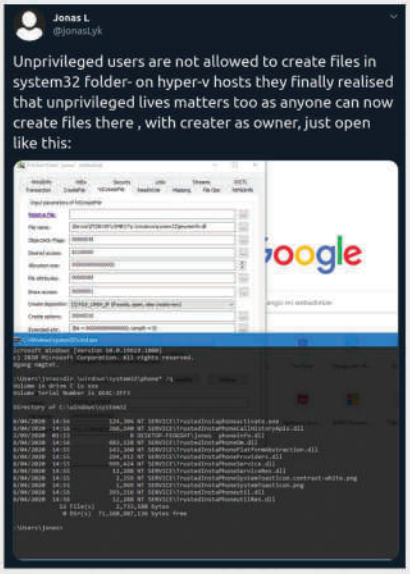
[1] Keylogger
[2] Restricted

بدون نگرانی از تحت تاثیر قرار گرفتن سیستم‌عامل خود برنامه‌ای را که به آن اعتماد ندارند، اجرا کنند یا وب‌سایتی مشکوکی را باز نمایند.

کاربران ویندوز ۱۰ باید توجه نمایند که مایکروسافت فعلا وصله‌ای برای این محصول ارائه نداده است.



برای نشان دادن این آسیب‌پذیری، Lykkegaard یک فایل خالی به نام phonein-fo.dll در system32/ ایجاد می‌کند؛ ایجاد هرگونه تغییر در این مکان به امتیاز دسترسی بالاتری نیاز دارد اما هنگام فعال بودن Hyper-V رعایت این محدودیت‌ها ضروری نیست.



از آنجا که سازنده فایل مالک، آن نیز می‌باشد، لذا مهاجم می‌تواند کد مخرب را در داخل آن قرار دهد تا هر زمان که نیاز داشت، با امتیاز دسترسی بالاتری، اجرا شود.

منبع خبر :

Scan Link

اخبار کوتاه

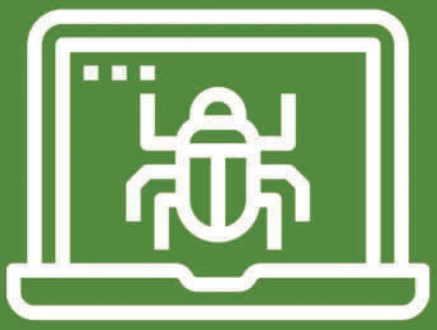
اتصال غیرمجاز هکر به دیوایس در پی آسیب‌پذیری جدید بلوتوث

سازمان متولی «بلوتوث» با انتشار بیانیه‌ای از کشف آسیب‌پذیری جدید در این فناوری ارتباطی بی‌سیم خبر داد. این آسیب‌پذیری که BLURtooth نام دارد، در پروتکل Cross-Transport Key Derivation یا به اختصار CTKD فناوری بلوتوث کشف شده است. از این پروتکل برای برقراری ارتباط و ایجاد کلیدهای احراز هویت (Authentication Keys) بین دو دیوایس بلوتوثی استفاده می‌شود. CTKD دو کلید احراز هویت متفاوت برای استاندارد بلوتوث کم انرژی (BLE) و استاندارد برد کوتاه BR/EDR می‌سازد. وظیفه این پروتکل آماده کردن کلیدهاست و انتخاب نوع مناسب را به دیوایس می‌سپارد.

حال طبق گزارشی که توسط گروه استانداردسازی بلوتوث (SIG) و دانشگاه کارنگی ملون منتشر شده، هکر می‌تواند با دستکاری پروتکل CTKD کلیدهای احراز هویت جعلی را جایگزین کلیدهای اصلی دیوایس کرده (Overwrite) و کنترل سرویس‌ها و اپلیکیشن‌های مبتنی بر بلوتوث دستگاه را در دست بگیرد.

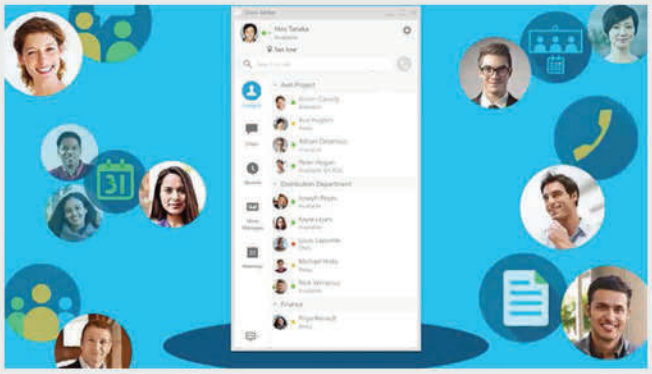
هکرها می‌توانند در حمله BLURtooth کلیدهای احراز هویت را به طور کامل جایگزین کرده و یا قدرت رمزگذاری کلیدهای اصلی را کاهش دهند. به گفته محققان تمام دیوایس‌هایی که از بلوتوث نسخه ۴.۰ و ۵.۰ استفاده می‌کنند، در برابر این حمله آسیب پذیرند. بلوتوث ۵.۱ دارای قابلیت‌های جدیدی است که پس از فعال شدن مانع از حملات BLURtooth می‌شود.

در حال حاضر از زمان دقیق انتشار بروزرسانی و همچنین تعداد دیوایس‌های آسیب پذیر در برابر BLURtooth اطلاعاتی در دست نیست. کد شناسایی این باگ CVE-2020-15802 است، بنابراین کاربران می‌توانند با بررسی بروزرسانی‌های نرم افزاری جدیدی که منتشر می‌شوند، نسبت به برطرف شدن آن آگاه شوند.



آسیب پذیری

نقص امنیتی موجود در ویدئو کنفرانس Jabber سیسکو



در پی نقص امنیتی موجود در نرم‌افزار ویدئو کنفرانس Jabber، شرکت سیسکو، نسخه جدیدی از این نرم‌افزار را برای سیستم‌عامل‌های ویندوز منتشر کرد که در این بروزرسانی، آسیب‌پذیری‌های موجود را وصله زد. تبعات ناشی از این آسیب‌پذیری ممکن است بسیار خطرناک باشد و در صورت بهره‌برداری از آن، احراز هویت مهاجم غیرمجاز تأیید شده و در نتیجه می‌تواند از راه دور کد دلخواه (RCE[1]) را اجرا کند. این نقص‌ها که توسط شرکت امنیتی Norwegian برطرف شده است، بر تمامی نسخه‌های کلاینت Jabber (۱۲.۹-۱۲.۱) تأثیر می‌گذارد.

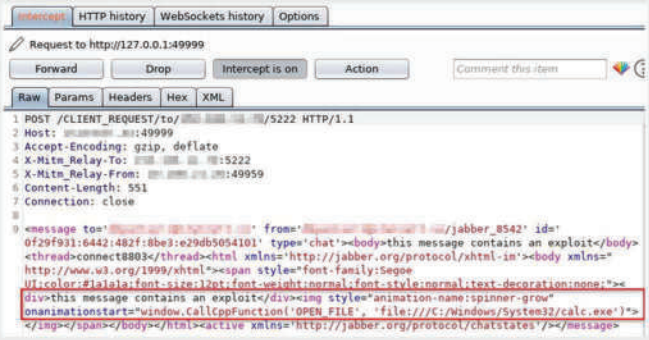
از بین نقص‌های امنیتی موجود، دو مورد از آن‌ها، با ارسال یک پیام ساختگی در مکالمات و چت‌های گروهی و مکالمات افراد خاص، بهره‌برداری شده و امکان اجرای کد از راه دور را به مهاجم خواهد داد.

شدیدترین و خطرناک‌ترین نقص امنیتی مربوط به آسیب‌پذیری با شناسه "CVE-2020-3495" است که به دلیل اعتبارسنجی نادرست محتویات پیام می‌باشد و می‌تواند با ارسال پیام مخرب و ساختگی Extensible Messaging and Presence Protocol (XMPP) به نرم‌افزار تحت تأثیر، توسط مهاجم مورد سوءاستفاده قرار گیرد. این نقص دارای امتیاز CVSS 9.9 و شدت بحرانی است.

بنا بر اظهارات منتشر شده از طرف شرکت سیسکو: بهره‌برداری موفق از این آسیب‌پذیری موجب خواهد شد تا اپلیکشن، برنامه‌های دلخواه را با سطح دسترسی حساب‌کاربری که در حال اجرای نرم‌افزار کلاینت Jabber می‌باشد، بر روی سیستم هدف اجرا کند و منجر به اجرای کد دلخواه شود. این نقص پس از هشدار سیسکو مبنی بر بهره‌برداری از نقص روز صفرم نرم‌افزار روتر IOS XR به وجود آمد.

XMPP (که Jabber نامیده می‌شود) یک پروتکل ارتباطی مبتنی بر XML است که جهت سهولت در امر پیام‌رسانی فوری بین دو یا چند شبکه استفاده می‌شود، این پروتکل به گونه‌ای طراحی شده است که توسعه‌پذیر بوده و امکان اضافه شدن قابلیت‌های جدید از جمله XEP-0071: XHTML-IM به آن وجود دارد. نقص Cisco Jabber در واقع ناشی از آسیب‌پذیری cross-site scripting به هنگام تجزیه و تحلیل پیام XHTML-IM می‌باشد.

[1] Remote Code Execution



بررسی نمی‌کند و در عوض آن‌ها را از طریق فیلتر XSS معیوب منتقل می‌کند؛ در نتیجه یک پیام مجاز XMPP، قطع و اصلاح شود و باعث خواهد شد تا اپلیکیشن، یک برنامه اجرایی دلخواه را که از قبل در مسیر فایل محلی اپلیکیشن وجود داشته را اجرا کند که برای این امر، از تابع آسیب‌پذیر Chromium Embedded Framework (CEF) یعنی یک فریمورک اوپن سورس که در مرورگر وب اپلیکیشن‌های دیگر استفاده می‌شود، بهره گرفته می‌شود. این امر می‌تواند توسط مهاجم مورد سوءاستفاده قرار گرفته و منجر به اجرای فایل "exe." در دستگاه قربانی شود.

بااین وجود، مهاجمان باید به دامنه‌های XMPP قربانی دسترسی داشته باشند تا جهت بهره‌برداری موفق از آسیب‌پذیری مذکور، پیام مخرب XMPP را ارسال کنند.

علاوه بر این، سه نقص دیگر با شناسه‌های "CVE-2020-3537"، "CVE-2020-3498" و "CVE-2020-3430"، می‌تواند جهت تزریق دستورات مخرب و افشای اطلاعات مورد بهره‌برداری قرار گیرند، از جمله پسورد هش شده NTLM کاربران.

✔ توصیه امنیتی

در پی شیوع ویروس کرونا و تمایل کاربران به استفاده از نرم‌افزارهای ویدئوکنفرانسی جهت برگزاری کنفرانس‌های خود به صورت مجازی و همچنین نظر به آن که بسیاری از اطلاعات حساس از طریق تماس‌های ویدئویی یا پیام‌های فوری به اشتراک گذاشته می‌شوند، امنیت این نرم‌افزارها از اهمیت بالایی برخوردار می‌باشد و لازم است که کاربرانِ نرم‌افزار Jabber جهت کاهش خطرهای احتمالی، نرم‌افزار خود را به جدیدترین نسخه و نسخه‌هایی که این آسیب‌پذیری در آن‌ها رفع شده است(یعنی 12.1.3 , 12.5.2, 12.6.3, 12.7.2, 12.8.3 و 12.9.1) بروزرسانی کنند.

منبع خبر :

Scan Link

رفع سه نقص امنیتی در وب‌سرور آپاچی

اخیراً سه آسیب‌پذیری با شناسه‌های "CVE-2020-9490"، "CVE-2020-11984" و "CVE-2020-11993"، در وب‌سرور آپاچی توسط Felix Wilhelm محقق امنیتی Google Project Zero کشف شد که دو مورد از آن‌ها دارای شدت بالا(Base Score 7.5) و یک مورد نیز دارای شدت بحرانی (Base Score 9.8) می‌باشد. در ادامه به بررسی هر یک از این آسیب‌پذیری‌ها پرداخته خواهد شد.

- **CVE-2020-9490**

به گفته Felix Wilhelm، ماژول Apache's mod_http2، از ویژگی خاصی پشتیبانی می‌کند که کلیه منابعی که قبلاً روی یک اتصال HTTP/2منتقل شده‌اند را نگه می‌دارد؛ همچنین کلاینت می‌تواند با ارسال این ویژگی رمزگذاری‌شده بر مبنای base64 در Cache-Digest header، از نگهداری غیرضروری منابع جلوگیری کند که از بین آسیب‌پذیری‌های مذکور، این آسیب‌پذیری با شدت بحرانی در ماژول HTTP/2 وجود دارد. این نقص تحت شرایط خاص، از طریق اجرای کد از راه دور یا حمله انکار سرویس مورد بهره‌برداری امنیتی قرار خواهد گرفت؛ گفتنی است که مهاجم می‌تواند با استفاده از Cache-Digest header دستکاری شده، باعث Crash در حافظه و انجام حمله منع سرویس[1] شود.

- **CVE-2020-11984**

آسیب‌پذیری با شناسه "CVE-2020-11984" با شدت بالا یک نقص مربوط به سرریز بافر می‌باشد که بر ماژول "mod_uwsgi" تأثیر می‌گذارد و می‌تواند منجر به اجرای کد از راه دور شود؛ این نقص به طور بالقوه می‌تواند به یک مهاجم اجازه دهد داده های حساس را بسته به امتیازات مرتبط با یک برنامه در حال اجرا بر روی سرور، مشاهده یا حذف کند و یا آن‌ها را تغییر دهد.

- **CVE-2020-11993**

آسیب‌پذیری با شناسه "CVE-2020-11993" نیز تنها هنگامی که debugging در ماژول "mod_http2" فعال است، قابل بهره‌برداری می‌باشد. این آسیب‌پذیری منجر خواهد شد تا اطلاعات ورود بر روی یک کانکشن اشتباه ایجاد و منجر به تخریب حافظه شود.

✔ توصیه امنیتی

اگر چه تاکنون گزارشی در خصوص بهره‌برداری از این آسیب‌پذیری‌ها منتشر نشده است، اما توصیه می‌شود کاربرانی که سایت‌هایشان از طریق وب‌سرور آپاچی اجرا می‌شود، هر

[1] remote code execution
[2] Escalation of Privileges

هر چه سریع‌تر وب‌سرور خود را به نسخه ۲.۴.۴۶ بروزرسانی کنند تا از گزند این سه آسیب‌پذیری در امان باشند؛ همچنین لازم است بررسی شود اپلیکشن، فقط با مجوزهای مورد نیاز، پیکربندی شده است تا احتمال خطر کاهش یابد.

منبع خبر :

Scan Link

رفع چندین آسیب‌پذیری مهم در تلفن‌هـــــای همراه سامسونگ

اخیراً شرکت سامسونگ برای رفع برخی آسیب‌پذیری‌های بحرانی موجود در تلفن‌های همراه خود، بروزرسانی‌های امنیتی منتشر کرد. این بروزرسانی‌های امنیتی شامل تعداد زیادی وصله امنیتی می‌باشد که همه آسیب‌پذیری‌های مهم در بسیاری از نسخه‌های سیستم‌عامل Android را برطرف می‌کند. با این حال، بروزرسانی امنیتی منتشر شده در سپتامبر سال ۲۰۲۰، شامل تلفن همراه مدل Galaxy Note 9 (SM-N960F) نیز خواهد شد.

براساس گزارش‌های منتشر شده، اولین بروزرسانی، برای رفع آسیب‌پذیری موجود در گوشی سامسونگ 5G منتشر شد. این آسیب‌پذیری به گونه‌ای عمل می‌کند که بدون داشتن مجوز، می‌توان از دستوالعمل‌های USB debugging مرتبط با دستورات LTE و 5G استفاده کرد.

در میان آسیب‌پذیری‌های موجود در گوشی‌های سامسونگ، شدیدترین آسیب‌پذیری دارای شناسه "CVE-2020-0240"، 8.8 Base Score و شدت بحرانی می‌باشد که به واسطه نقص "integer overflow" موجود در سیستم‌عامل اندروید، منجر به اجرای کد از راه دور خواهد شد؛ به گفته محققان، این آسیب‌پذیری موجب می‌شود تا یک مهاجم از راه دور اختیارات کامل دستگاه شما را در بدست بگیرد. آسیب‌پذیری‌های دیگری نیز وجود دارد که این امکان را به مهاجم خواهند داد تا ارتباط کاربر را جهت کسب مجوز آنتن هوایی دور بزند و با قدرت بالاتری کد را مدیریت کند.

در صورت بهره‌برداری از آسیب‌پذیری با شدت بحرانی این اماکن فراهم خواهد شد که به یک برنامه مخرب اجازه داده شود تا به راحتی ارتباط کاربر را جهت بدست آوردن دسترسی‌های بیشتر دور بزند.

در جداول زیر، دیگر آسیب‌پذیرهایی که در بروزرسانی منتشر شده رفع شده‌اند را مشاهده می‌کنید.

- **Framework**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0240	RCE[1]	بالا	10
CVE-2020-0238	EoP[2]	بالا	8.0, 8.1, 9, 10
CVE-2020-0257	EoP	بالا	10
CVE-2020-0239	ID	بالا	9, 10
CVE-2020-0249	ID	بالا	8.0, 8.1, 9, 10
CVE-2020-0258	ID	بالا	10
CVE-2020-0247	DoS	بالا	8.0, 8.1, 10

- **Media Framework**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0241	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0242	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0243	EoP	بالا	8.0, 8.1, 9, 10

- **System**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0108	EoP	بالا	8.1, 9, 10
CVE-2020-0256	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0248	ID	بالا	10
CVE-2020-0250	ID	بالا	10

در خصوص گوشی‌های مدل Galaxy شرکت سامسونگ، انتشار بروزرسانی‌ها آغاز شده است و آخرین وصله امنیتی برای تاریخ ۲۰۲۰/۰۸/۰۱ ثبت شده است، که این مسئله نشان می‌دهد آسیب‌پذیرهایی که منجر به افزایش سطح دسترسی (EoP) می‌شوند و با بروزرسانی امنیتی منتشر شده در تاریخ ۲۰۲۰/۰۸/۰۵ وصله شده‌اند، هنوز هم قابل بهره برداری می‌باشند.

آسیب‌پذیری با شناسه "CVE-2020-0259" و Base Score 7.8 نیز می‌تواند یک مهاجم محلی را قادر سازد که با افزایش تمام امتیازات ، کد دلخواه خود را بر روی دستگاهی که وصله نشده است اجرا کند و منجر به افزایش سطح دسترسی خود شود.

✔ توصیه امنیتی

کارشناسان به کابرانی که از گوشی‌های سامسونگ استفاده می‌کنند توصیه کردند که هر چه سریع‌تر دستگاه‌های اندرویدی خود را بروزرسانی کنند تا از گزند این آسیب‌پذیری‌ها در امان باشند، همچنین کاربران باید از فعال بود گزینه "بروزرسانی خودکار" در گوشی خود، اطمینان حاصل کنند.

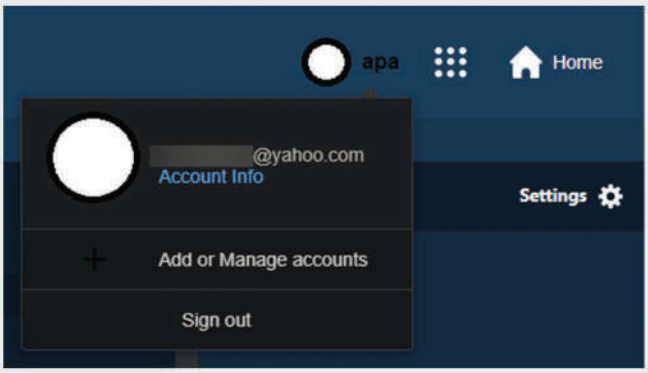
منبع خبر :

Scan Link

[1] remote code execution
[2] Escalation of Privileges

مقالات آموزشی

چند راهکار برای حفظ امنیت حساب کاربری یاهو

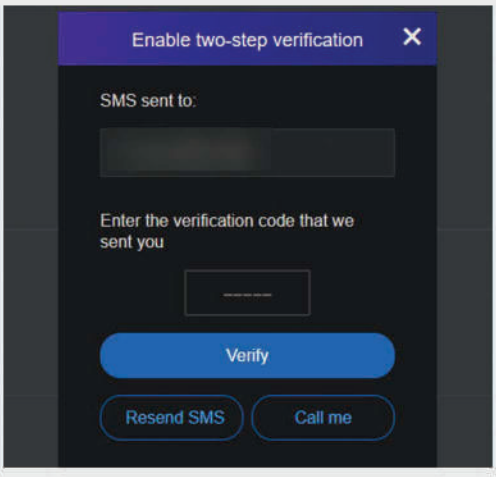


۱. رمز قوی انتخاب کنید

انتخاب رمز عبور قوی یکی از عوامل مهم در تأمین امنیت حساب کاربری یاهو می‌باشد. ایمیل شما یک حساب کاربری بسیار مهم است که توسط آن وارد سرویس‌های دیگر می‌شوید. اگر فرد غیرمجاز وارد ایمیل یاهوی شما شود می‌تواند سوء استفاده‌های زیادی در راستای اهداف خود انجام دهد.

۲. فعال کردن تأیید هویت دومرحله‌ای

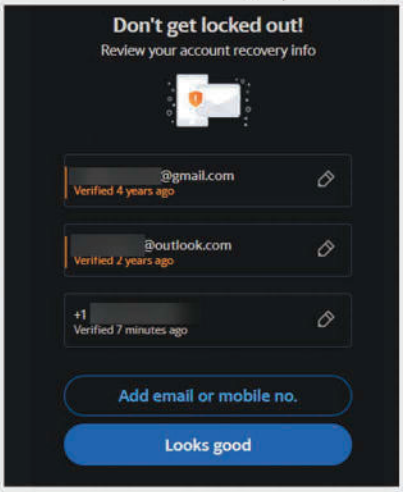
احراز هویت دو مرحله‌ای یک ویژگی امنیتی مهم است که می‌تواند امنیت حساب شما را حتی اگر هکرها رمز عبور شما را سرقت کنند حفظ کند. احراز هویت دومرحله‌ای را برای هر حساب کاربری یاهو خود فعال کنید این کار باعث می‌شود که در زمان ورود به حساب کاربری خود از یک دستگاه جدید از سرویس آنلاین درخواست یک کد یکبار مصرف نماید و آن را از طریق پیام متنی، تماس تلفنی، ایمیل یا توسط یک برنامه گوشی همراه برای کاربر ارسال کند. این کد علاوه بر رمز عبور معمولی کاربر لازم است، یاهو همچنین دارای یک ویژگی به نام Account Key است که به طور کامل روند مرسوم رمزهای عبور را کنار می‌گذارد و از طریق تلفن همراه باید ورود به سیستم را تأیید نمایید.



۳. اطلاعات ریکاوری خود را آپدیت کنید

در مواقعی که رمز خود را فراموش کردید و قادر به ورود به حساب کاربری نمی‌باشید با

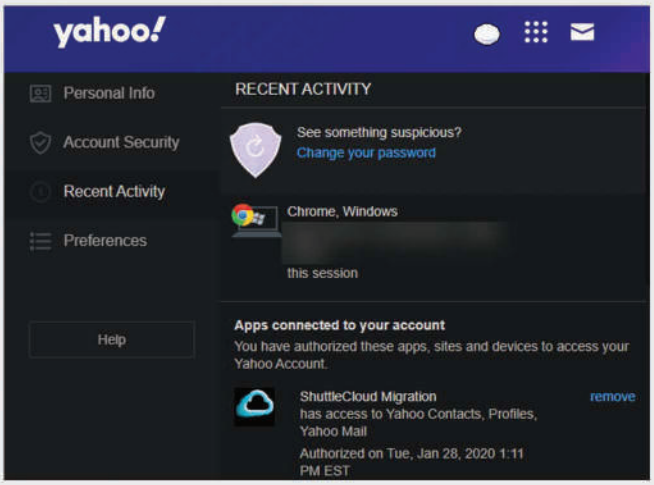
استفاده از اطلاعات تماس برای ورود به حساب خود از یک آدرس ایمیل دیگر و یا شماره تلفن که از قبل وارد کرده‌اید اقدام نمایید.



۴. بررسی تاریخچه حساب کاربری

یاهو همیشه خلاصه‌ای از فعالیت‌هایتان را به شما می‌دهد. به این وسیله اگر کسی وارد حساب شما شود متوجه خواهید شد.

روی Account Info کلیک کرده و تب Recent activity را باز کنید. سپس لیستی از فعالیت‌هایتان را مشاهده خواهید کرد که نام سیستم‌عامل و مرورگری که با آن وارد حساب شده‌اید را به شما نمایش می‌دهد. با کلیک کردن روی لیست می‌توانید فعالیت سی روز خود، آدرس IP و مکان ورود را ببینید.



۵. مواظب ایمیل‌های فیشینگ باشید

نقص‌های بزرگ داده معمولاً به همراه ایمیل فیشینگ است، زیرا هکرهای سایبری تلاش می‌کنند تا از منافع عمومی در چنین حوادثی استفاده کنند. این ایمیل‌ها می‌توانند به عنوان هشدارهای امنیتی ارسال شوند، می‌توانند شامل دستورالعمل‌هایی برای دانلود برنامه‌های مخرب باشند که به عنوان ابزار امنیتی معرفی می‌شوند و یا می‌توانند کاربران را به وب‌سایت هایی منتقل کنند که برای "تأیید" حساب‌ها، اطلاعات بیشتری را از کاربران درخواست نمایند.

اطمینان حاصل کنید که هر دستورالعملی که در پاسخ به یک حادثه امنیتی برای شما ارسال شده است

از طرف ارائه دهنده خدمات و یا یک منبع قابل اعتماد باشد. ایمیل‌های رسمی یاهو در رابط ایمیل یاهو به راحتی قابل شناسایی هستند زیرا آنها با یک آیکون Y بنفش مشخص شده‌اند.

حتی‌الامکان از پاسخ‌های درست به سوالات امنیتی اجتناب کنید. پاسخی اشتباه در نظر بگیرید و از آن به عنوان پاسخ استفاده کنید. در واقع، یاهو حتی توصیه نمی‌کند که از سؤالات امنیتی استفاده کنید، بنابراین می‌توانید به تنظیمات امنیتی حساب کاربری خود بروید و آنها را حذف کنید.

اخبار کوتاه

صفحات فیشینگ جدید برای به دام انداختن کارمندان شرکت‌های معتبر

فیشرها صفحات فیشینگ را این بار در سایت‌های معتبر مشاغل مختلف ایجاد کرده‌اند و از آن برای پنهان کردن حمله و فریب کارمندان برای ارائه اطلاعات آن‌ها استفاده می‌کنند. نکته قابل توجه در این روش این است که در مرحله لود، صفحه کاملا قانونی شرکت بارگذاری می‌شود، سپس فیلدهای جعلی فیشینگ در بالای صفحه برای ورود اطلاعات کارمندان پدیدار می‌شود.

این حمله با ارسال یک ایمیل، موضوع مسدود شدن برخی پیام‌های ارسالی از طرف شرکت را خبر می‌دهد که ادعا می‌شود از طرف تیم پشتیبانی فنی شرکت است. برای ایجاد احساس فوریت برای وارد شدن کاربران، در موضوع این ایمیل درج شده است که ایمیل‌های مسدودی شما برای حذف برنامه‌ریزی شده‌اند، مگر اینکه گیرنده، آن‌ها را بررسی کند و برای بازیابی آن‌ها اقدامی انجام دهد.

پس از باز کردن ایمیل ارسالی توسط کاربر، یک لینک پیوند در متن ایمیل، قربانی را به صفحه فیشینگی می‌برد که در آن، صفحه اصلی شرکت بر اساس نام دامنه در آدرس به طور خودکار بارگیری شده است و همه چیز را طبیعی و واقعی جلوه می‌دهد.

گرچه ممکن است این روش در شرکت‌های کوچکتر موفقیت‌آمیز نباشد، اما در محیط‌های بزرگتر که کارمندان احتمالاً بیشتر به سیستم‌های محافظت از ایمیل اعتماد می‌کنند و هوشیاری کمتری دارند، کارآمد است.

برگزاری وبینار رایگان امن‌سازی ایمیل و سرویس‌های ایمیل

ارسال ایمیل از طریق سرویس‌های اینترنتی رایگان نظیر جیمیل، یاهو و سایر سرویس دهنده‌های ایمیل، به یک امر رایج برای ارتباط بین کاربران معمولی تبدیل شده است و حتی افراد سرشناس، سیاستمداران، کارمندان و مدیران مشاغل و کسب و کارهای حساس نیز از این سرویس‌ها برای ارسال پیام استفاده می‌کنند. اما آیا این سرویس‌های رایگان از امنیت کافی برای حفاظت از حریم خصوصی کاربران و اطلاعات شخصی آن‌ها برخوردار هستند؟ برای پاسخ به این سوال و سپس راهکارهای امن کردن ایمیل، مرکز تخصصی آپا اقدام به برگزاری وبینار رایگان امن‌سازی ایمیل و سرویس‌های ایمیل در مورخ ۵ شهریور ماه ۱۳۹۹ با شرکت پرسنل سازمان‌ها، شرکت‌های خصوصی، دانشجویان و علاقمندان نمود.

برگزاری وبینار رایگان دفاع لایه‌ای در شبکه - دفاع در عمق

دفاع در عمق، یک مدل حفاظتی لایه‌ای برای اجزاء مهم سیستم‌های اطلاعاتی است. استراتژی دفاع در عمق محدوده‌های حفاظت از شبکه و زیرساخت، حفاظت و دفاع در عمق محدوده‌های حفاظت از شبکه و زیرساخت، حفاظت و دفاع در محدوده‌های مرزی (نقطه تماس شبکه با سایر شبکه‌ها) و حفاظت و دفاع از محیط محاسباتی و عملیاتی را شامل می‌شود.

ایده اصلی که پشت این مفهوم وجود دارد این است که اگر یکی از اقدامات پیشگیرانه شما در برابر نفوذ به شبکه‌تان موفق نبود، سدهای دیگری از موانع امنیتی وجود داشته باشند که به مانند گارد امنیتی چند لایه، امنیت شبکه شما را تضمین کنند. Defense in depth سرعت حمله یک مهاجم را کاهش می دهد و تلاش او برای عبور از لایه‌های مختلف امنیتی که شما در شبکه‌تان اجرا کردید، وقت کافی را به شما خواهد داد تا حمله را شناسایی و متعاقباً با آن برخورد کنید. در همین راستا مرکز تخصصی آپا دانشگاه رازی وبیناری به منظور آشنایی با روش‌های دفاع لایه‌ای در شبکه در مورخ ۱۹ شهریور ماه ۱۳۹۹ با شرکت پرسنل سازمان‌ها، شرکت‌های خصوصی، دانشجویان و علاقمندان برگزار نمود.

ثبت‌نام دوره‌هـــــای آنلاین پاییزی مرکز تخصصی آپا

مرکز آپا دانشگاه رازی با توجه به شرایط کنونی کشور اقدام به برگزاری دوره‌های آموزشی آنلاین نموده است. در این فصل از برگزاری دوره‌های آموزشی، ثبت‌نام چهار دوره پیکربندی شبکه CCNA(New)، پیکربندی سوییچ‌های سیسکو CCNP Switch(New)، مقدماتی امنیت شبکه Security+ و دوره بازرس امنیت شبکه Systems and Network Auditor آغاز گردید. جزییات هر یک از دوره‌ها به صورت کامل در لینک زیر ذکر شده است.

لینک ثبت‌نام:

Scan Link


دوره‌های آنلاین پاییزی مرکز آپا دانشگاه رازی
با اساتیدی مجرب
دارای مدارک بین المللی
همراه با ارائه مدرک معتبر افتا
۲۵ درصد تخفیف ویژه دانشجویان
تخفیف پلکانی
برای دانش‌پذیران قدیمی دوره های آپا
با همکاری انجمن علمی مهندسی کامپیوتر
دوره پیکربندی شبکه CCNA (NEW)
طول دوره
۶۰ ساعت
روز و ساعت
دوشنبه‌ها ۱۷:۳۰ الی ۲۰
مدرس
مهندس آرزو حسنی
CISCO CERTIFIED CCNA ROUTING & SWITCHING
دوره پیکربندی سوییچ‌های سیسکو CCNP Switch (NEW)
طول دوره
۵۰ ساعت
روز و ساعت
چهارشنبه‌ها ۱۶ الی ۲۰
مدرس
مهندس مهدی اسفندیاری
CISCO CERTIFIED CCNP SWITCHING
دوره مقدماتی امنیت شبکه Security+
طول دوره
۴۰ ساعت
روز و ساعت
یکشنبه‌ها ۱۷:۳۰ الی ۲۰
مدرس
مهندس مهدی فرهمند
CompTIA Security+
دوره بازرس امنیت شبکه Systems and Network Auditor(GSNA)
طول دوره
۵۰ ساعت
روز و ساعت
دوشنبه ها ۹ الی ۱۲
مدرس
مهندس حسین ملک راده
GSNA
لینک ثبت نام
evand.com/events/aparazi-99
مهلت ثبت نام تا ۲۳ مهر ماه ۱۳۹۹
راه های ارتباطی
@APA_Razi
@APARazi
۰۸۳۳۴۳۴۳۲۵۱

مرکز تخصصی آپا دانشگاه رازی