بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیستم

اردیبهشت ماه ۱۳۹۹

ادامه آسیب‌پذیری‌ها در افزونه‌های محبوب وردپرس

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری
سیده آرزو حسنی

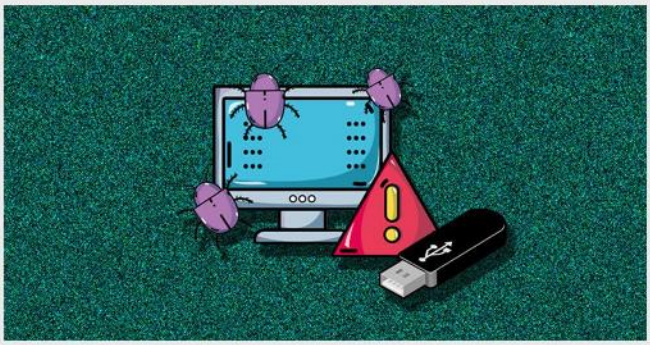
صفحه آرایی: **سید احسان حسینی**

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

استخراج ارز دیجیتال از طریق درایوهای مخرب USB

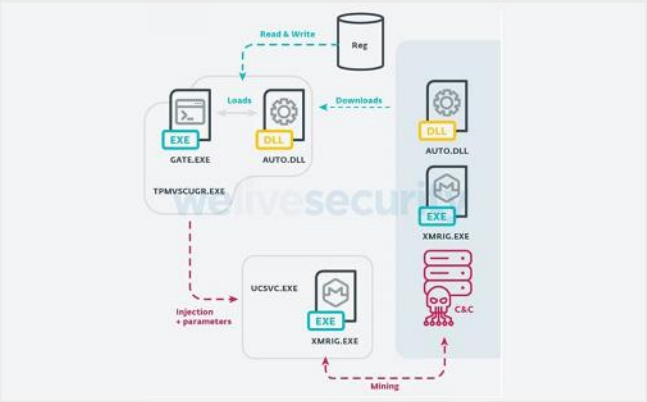


محققان امنیتی ESET اعلام کردند که بخشی از یک بات‌نت بدافزار به نام "VictoryGate" که از سال 2019 شروع به فعالیت کرده است، حداقل 35,000 سیستم ویندوز را آلوده کرده است و به دنبال آن مهاجمان به صورت مخفیانه اقدام به استخراج ارز دیجیتال Monero کرده‌اند.

به گفته‌ی ESET، فعالیت اصلی این بات‌نت، استخراج ارز دیجیتال Monero می‌باشد و قربانیان آن، سازمان‌های خصوصی و دولتی و موسسات مالی هستند.

ESET اذعان داشت که این فرآیند مخرب از طریق ارائه دهنده DNS داینامیک و بدون IP، کار خود را پیش می‌برد تا سرورهای کنترل-فرمانِ (C&C) مخرب را مختل و دامنه‌های جعلی (aka sinkholes) را جهت نظارت بر فعالیت بات‌نت راه‌اندازی کند. داده‌های sinkhole نشان می‌دهد که در ماه‌های فوریه و مارس سال جاری، روزانه بین 2000 تا 3500 کامپیوتر آلوده، به سرورهای کنترل-فرمان متصل بوده‌اند.

به گفته محققان ESET، ماژول VictoryGate از طریق دستگاه‌هایی که قابلیت جابجا شدن دارند (مانند درایوهای USB)، در سیستم قربانی پخش شده و هنگام اتصال به دستگاه مورد هدف، پی‌لود مخربی را بر روی آن نصب خواهد کرد.



به علاوه این که این ماژول جهت دریافت پی‌لود ثانویه، با سرور C&C ارتباط برقرار می‌کند تا کد دلخواه را به فرآیندهای مجاز ویندوز تزریق کند، مانند نرم‌افزار استخراج ارز XMRig در فرآیند ucsvc.exe یا

برای تسهیل استخراج ارز Monero.

از داده‌های جمع‌آوری شده در طول فعالیت‌های sinkholing، می‌توان تعیین کرد که به طور متوسط 2,000 دستگاه در طول روز مورد حمله استخراج ارز قرار می‌گیرند. اگر متوسط نرخ هش را، 150 هش در ثانیه تخمین بزنیم، می‌توان گفت که مهاجمان حداقل 80 Monero، یعنی تقریباً 6000 دلار، به تنهایی از طریق این بات‌نت جمع‌آوری کرده‌اند.

ESET همچنین در خصوص آلودگی‌های جدیدی که ممکن است در آینده از طریق درایورهای USB رخ دهند هشدار داد اما با وجود آن که بخش‌های مختلفی از زیرساخت‌های سرورهای C&C دچار مشکل شده‌اند، نمی‌توانند پی‌لودهای ثانویه را دریافت کنند.

باتوجه به آن که botmaster در هر زمان می‌تواند عملکرد پی‌لودهایی که بر روی دستگاه های آلوده، دانلود و اجرا شده‌اند را جهت انجام فعالیت مخرب بروزرسانی کند، این مسئله خطر را جدی‌تر خواهد کرد.

منبع خبر :

https://thehackernews.com/2020/04/usb-drive-botnet-malware.html

Scan Link

وصله آسیب‌پذیری روز صفرم SQL Injection و Code Execution در فایروال Sophos

یک آسیب‌پذیری SQL injection در محصول فایروال XG خود را که توسط مهاجمان در سراسر دنیا مورد اکسپلویت قرار گرفته بود، وصله کرد.

این شرکت در تاریخ 22 آوریل 2020، از این نقص در فایروال خود مطلع گشت و براساس بررسی‌های انجام شده بیان کرد که هکرها می‌توانند سیستم‌هایی با رابط کاربری administration (HTTPS admin service) و یا پورتال کاربری در معرض منطقه WAN را مورد حمله قرار دهند.

همچنین فایروالی که به صورت دستی پیکربندی شده باشد و پورتی مشابه admin یا User Porta را به اشتراک می‌گذارد نیز تحت تاثیر این آسیب‌پذیری قرار می‌گیرد.

یک مهاجم می‌تواند از آسیب‌پذیری pre-auth SQL injection برای دستیابی به دستگاه‌های فایروال XG، سوء استفاده کرده و با استفاده از این نقص، یک فایل مخرب را بر روی دستگاه بارگیری کند.

مهاجم به کمک این کد مخرب می‌تواند نام‌های کاربری و رمزهای عبور هش شده را از هر حساب کاربری محلی دریافت کند. این حساب‌های کاربری شامل حساب‌های کاربری admin لوکال دستگاه، حساب‌های پورتال کاربر و حساب‌هایی است که برای دسترسی از راه دور یا remote استفاده می‌شوند. رمزهای عبور مرتبط با سیستم‌های احراز هویت خارجی مانند(AD) Active Directory یا LDAP در معرض خطر قرار ندارند.

طبق اظهارات شرکت Sophos، هیچ نشانه‌ای مبنی بر دسترسی مهاجمان به شبکه محلی خارج از دستگاه‌های فایروال XG وجود ندارد. پس از تشخیص مؤلفه‌ها و تاثیر حمله، Sophos یک عیب‌یاب (hotfix) را در تمامی نسخه‌های XG Firewall/SFOS پشتیبانی شده خود، مستقر ساخت.

هدف از این hotfix رفع آسیب‌پذیری SQL injection و جلوگیری از سوء استفاده بیشتر از آن است که فایروال XG را از دسترسی به زیرساخت‌های هر مهاجم متوقف کرده و تمام بقایای حمله را از بین برده است.

به کاربران توصیه می‌شود به منظور رفع این آسیب‌پذیری، hotfix را بر روی دستگاه خود اعمال نمایند و در دستگاه‌های در معرض خطر، رمزهای عبور تمام حساب‌های کاربری محلی مجددا تنظیم و reset شوند.

آسیب‌پذیری مذکور، تمام نسخه‌های Sophos XG Firewall firmware بر روی هر دو فایروال فیزیکی و مجازی را تحت تاثیر قرار می‌دهد. این شرکت hotfix (SFOS 17.0, 17.1, 17.5, 18.0) را نیز در اختیار کاربران قرار می‌دهد. به کاربرانی که از نسخه‌های قدیمی استفاده می‌کنند توصیه می‌شود آن را به جدیدترین نسخه ارتقاء دهند.

منبع خبر :

https://gbhackers.com/sophos-xg-firewall/

Scan Link

سرقت اطلاعات مهم کاربران توسط بدافزار اندرویدی EventBot!

محققان امنیتی از بدافزار اندرویدی به نام EventBot پرده برداشتند که اطلاعات بانکی کاربران، داده‌های شخصی آن‌ها و اطلاعات دریافت شده از طریق صفحه کلید را از دستگاه آن‌ها به سرقت می‌برد.

این بدافزار که نوعی تروجان است، در وهله‌ی اول از ویژگی Accessibility اندروید سوءاستفاده کرده و دیتاهای اپلیکیشن‌های مالی و SMSهای موجود بر روی دستگاه را به سرقت برده و همچنین SMSهای دریافتی را جهت دورزدن 2FA می‌خواند.

بدافزار EventBot طیف گسترده‌ای از 200 اپلیکیشن مالی مختلف از جمله اپلیکیشن‌های بانکداری، سرویس‌های انتقال پول و کیف پول‌های ارز دیجیتال[1] را مورد هدف قرار می‌دهد.

تروجان EventBot پس از به خطر انداختن این اپلیکیشن‌ها، دسترسی گسترده‌ای به داده‌های شخصی و تجاری خواهد داشت که حدود 60 درصد از دستگاه‌های اندرویدی را شامل می‌شود.

EventBot کاملاً جدید بوده در سال 2020 به یک بدافزار بزرگ موبایل تبدیل شده است و عاملان آن، نسخه‌های مختلفی (0.0.0.1، 0.0.0.2، 0.3.0.1، 0.4.0.1) از این بدافراز با ویژگی‌های گوناگون ایجاد کرده‌اند.

فرآیند کاری EventBot

همانطور که در تصویر زیرمشاهده می‌کنید، در ابتدا مهاجمان بدافزار را به عنوان یک اپلیکیشن کاربردی مجاز، با چند آیکن مختلف در فروشگاه‌های APK و سایر وب سایت‌های مشکوک بارگذاری می‌کنند.

پس از نصب ماژول مخرب، مجوزهای زیر از دستگاه قربانی درخواست می‌شود:

SYSTEM_ALERT_WINDOW - ایجاد پنجره‌هایی که در بالای سایر اپلیکیشن‌ها نشان داده می‌شود

READ_EXTERNAL_STORAGE - خواندن از حافظه‌ی اکسترنال یا خارجی

REQUEST_INSTALL_PACKAGES - درخواست نصب پکیج‌ها

INTERNET - باز کردن سوکت‌های شبکه

REQUEST_IGNORE_BATTERY_OPTIMIZATIONS - قرار دادن اپلیکشن در لیست سفید و نادیده گرفتن بهینه‌سازی باتری

WAKE_LOCK - جلوگیری از sleep پردازنده و کم نور شدن صفحه

ACCESS_NETWORK_STATE - دسترسی اپلیکیشن به اطلاعات مربوط به شبکه

REQUEST_COMPANION_RUN_IN_BACKGROUND - اجرای اپلیکیشن در پس‌زمینه

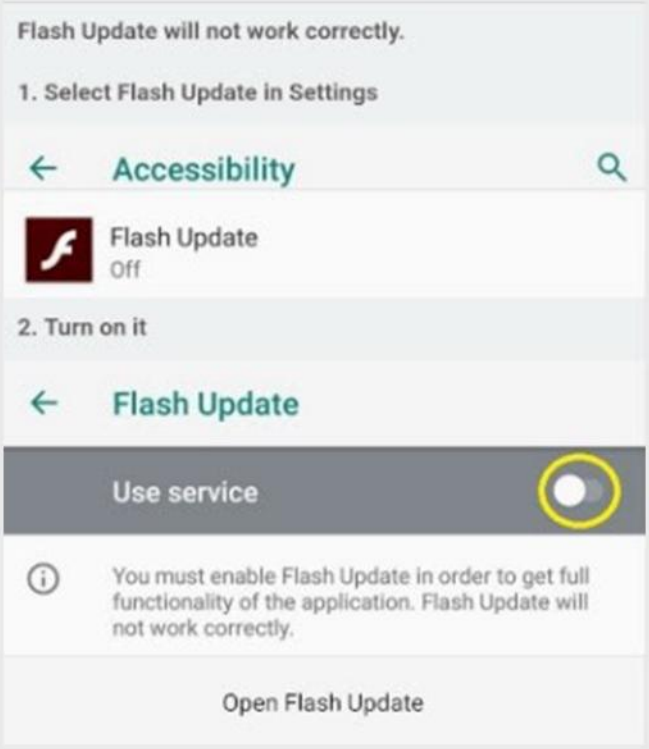
REQUEST_COMPANION_USE_DATA_IN_BACKGROUND- استفاده از داده‌ها در پس‌زمینه

RECEIVE_BOOT_COMPLETED - پس از بوت شدن، سیستم خود را راه اندازی کند که بدافزار EventBot از این مجوز جهت پایداری و اجرا در پس‌زمینه به عنوان یک سرویس، استفاده می‌کند.

RECEIVE_SMS - دریافت پیام‌های متنی

READ_SMS - خواندن پیام‌های متنی

همانطور که در تصویر زیر مشاهده می‌کنید، سپس این بدافزار کاربران را مجبور به اخذ مجوز دسترسی کرده تا به عنوان یک keylogger[2] به notification سایر اپلیکیشن‌های نصب شده بر روی دستگاه دسترسی داشته باشد.



[1] «والت» یا همان کیف پول ارز دیجیتال یک برنامه نرم‌افزاری است که کلیدهای خصوصی و عمومی را ذخیره می‌کند و با بلاک چین‌های مختلف در تعامل است تا کاربران بتوانند ارز دیجیتال خود را بفرستند، دریافت کنند و بر تراز حساب خود نظارت داشته باشند.

[2] کی‌لاگر، به نرم‌افزارهایی گفته می‌شود که کلیدهای فشرده‌شده بر روی صفحه کلید را ذخیره می‌کنند به صورتی که می‌توان از آن، اطلاعات تایپ شده کاربران از قبیل رمزهای عبور آن‌ها را سرقت کرد.

همچنین کاربر را مجبور به اخذ مجوز برای اجرای اپلیکیشن در پس‌زمینه دستگاه و ارتقاء آن به جدیدترین نسخه اندروید خواهد کرد!

براساس تحقیقات Cybereason:"این نسخه از بدافزار شامل 185 اپلیکیشن مختلف، از جمله اپلیکیشن‌های رسمی بانک‌های جهانی می‌باشد."

تهیه لیستی از کلیه‌ی اپلیکیشن‌هـــای نصب شده:

پـــس از نصب EventBot، کلیه‌ی برنامه‌های موجود در دستگاه هدف لیست کـــرده و آن‌ها را به سرور C2 ارسال می‌کند.

اطلاعات دستگاه:

EventBot اطلاعات دستگاه از جمله سیستم‌عامل، مدل و غیره را به C2 ارسال می‌کند.

رمزگذاری داده‌ها:

در نسخه‌ی اولیه EventBot، داده‌های استخراج شده با استفاده از تابع Base64 و RC4 رمزگذاری می‌شوند.

ربودن SMS :

EventBot امکان تجزیه متن SMS با استفاده از نسخه‌ی SDK دستگاه هدف را برای تجزیه و تحلیل درست آنها دارد.

هر نسخه از این بدافزار دارای قابلیت‌های منحصر به فردی در زمینه سرقت اطلاعات مالی می‌باشد، از جمله سرقت تراکنش‌ها و داده‌های شخصی، گذرواژه‌ها، اطلاعات وارد شده از طریق صفحه کلید و اطلاعات بانکی.

پیشنهادات امنیتی کارشناسان در این خصوص

- نرم‌افزارهای موجود بر روی دستگاه خود را همیشه به آخرین نسخه‌ی موجود به روزرسانی کرده و آن‌ها را از منابع مجاز از جمله Google Play دریافت کنید.
- همیشه دقت داشته باشید که مجوزها را تنها در صورت لزوم، بر روی دستگاه خود فعال کنید.
- در صورت مشکوک بودن اپلیکیشن، امضای APK را چک کرده و پیش از نصب، حتماً آن را بررسی کنید.
- برای برقراری امنیت بیشتر در دستگاه خود، از راه حل های شناسایی تهدید تلفن همراه استفاده کنید.

منبع خبر :

https://gbhackers.com/android-malware-eventbot/

Scan Link

اخبار کوتاه

مراقب کلاهبردارانی که تظاهر می‌کنند رابط سازمان بهداشت جهانی هستند، باشید.

این روزها کلاهبرداران سایبری از ویروس همه‌گیر کوید 19 سوءاستفاده کرده و با ارسال ایمیل و پیام‌های جعلی در واتس‌اپ، سعی در فریب کاربران و تحریک آن‌ها مبنی بر باز نمودن لینک‌ها و پیوست‌های ارسالیشان دارند که با باز کردن آن‌ها، نام‌کاربری و رمزعبور کاربران نمایش داده می‌شود و می‌توانند از آن‌ها جهت سرقت پول یا اطلاعات حساس استفاده کنند، لذا در این خصوص سازمان بهداشت جهانی توصیه کرده است که کاربران هشیار باشند که برای دسترسی به اطلاعات سلامتشان، هرگز نام‌کاربری یـــا رمزعبور از آن‌ها سؤال نخواهد شد و هرگز به سایتی جز www.who.int و یا دیگرسایت‌های معتبر مراجعه نکنند.

مراقب روش جدید کلاهبرداری پیامکی در واتس‌اپ باشید

ارسال پیام‌هایی حاوی لینک‌های ناشناس که افراد را به سایت‌های جعلی هدایت می‌کنند، یکی از روش‌هایی است که مجرمین سایبری برای سرقت اطلاعات و یا دسترسی و کنترل حساب کاربری شهروندان از آن استفاده می‌کنند. نکته‌ای که باید دقت کرد آن است که این پیام کلاهبرداری در خصوص شبکه اجتماعی اینستاگرام بوده ولی در پیام‌رسان واتس‌اپ ارسال می‌شود. کاربران دقت کنند به هیچ عنوان به پیام‌های دریافتی از شماره‌های ناشناس اعتماد نکرده و به لینک‌هایی که در اینگونه پیام‌ها ارائه می‌شود نیز مراجعه نکنند.

سرقت رمز حساب‌های بانکی و اطلاعات شخصی توسط بدافزار اندرویدی

نوع جدیدی از بدافزارهای اندرویدی به نام EventBot کشف شده است که می‌تواند به اطلاعات مهم کاربر، اطلاعات سیستم و داده‌های ذخیره شده در برنامه‌های دیگر دسترسی پیدا کند و به ربودن رمز و اطلاعات حساب‌های بانکی، پیامک‌ها، کدهای احراز هویت بپردازد، لذا توصیه می‌شود نرم‌افزارهای موجود بر روی دستگاه تلفن خود را به روز نگه دارید و آن‌ها را از منابع غیررسمی یا غیرمجاز بارگیری نکنید، اکثر برنامه‌های مجاز اندروید در فروشگاه Google Play در دسترس هستند.

اطلاعات مربوط به ۹۱ میلیون کاربـــــــر Tokopedia در وب تاریک فروخته شد

این بار هکرها Tokopedia را هدف قرار داده و توانستند به اطلاعات شخصی مربوط به 91 میلیون کاربر دسترسی پیدا کنند و آن‌ها را در وب‌تاریک به قیمت 5000 دلار به فروش برسانند. خبر بد برای کاربران Tokopedia این است که ظاهراً شرکت با نقض گسترده اطلاعات روبرو شده و داده‌های شخصی کاربرانش در معرض خطر قرار گرفته است. این اطلاعات شامل جنسیت، محل، نام‌کاربری، نام و نام خانوادگی، آدرس ایمیل، شماره تلفن ها و رمز عبور hashed می‌باشد. Hackread.com توصیه می‌کند که اگر در Tokopedia حساب کاربری دارید فوراً رمزعبور آن را تغییر دهید، همچنین گذرواژه ایمیل خود را نیز تغییر داده و نسبت به هرگونه فعالیت غیر عادی در حساب خود حساس باشید.

آسیب پذیری

آسیب‌پذیری بحرانی SaltStack Salt و تاثیر بر روی هزاران دیتاسنتر و محیط‌های ابری

فریمورک مدیریت Salt که توسط SaltStack توسعه یافته است، یک ابزار پیکربندی است که برای نظارت و بروزرسانی سرورها در دیتاسنتر و محیط‌های ابری مورد استفاده قرار می‌گیرد.

چندین آسیب‌پذیری بحرانی در Salt، به مهاجمان اجازه می‌دهد تا توکن‌های کاربران را از salt-master بازیابی کنند و دستورات دلخواه خود را در salt minions اجرا نمایند.

این آسیب‌پذیری‌ها که توسط محققان امنیتی F-Secure در نسخه‌های 2019.2.4 و 3000 این فریمورک کشف و شناسایی شدند، به مهاجمی که از راه دور درخواست اتصال به سرور را می‌دهد اجازه می‌دهد تمام مکانیسم‌های تصدیق هویت را دور بزند و پیام‌های کنترل دلخواه خود را منتشر کند و فایل‌ها را در هر مکانی در سیستم فایل اصلی بخواند و بنویسد.

مهاجمان همچنین می‌توانند کلیدهای محرمانه را به سرقت برده و به عنوان کاربر اصلی تصدیق هویت کنند که این اقدام منجر به اجرای کامل دستورات از راه دور با سطح دسترسی root در تمام minionsهای متصل شده به آن می‌گردد.

یکی از این آسیب‌پذیری‌ها با شناسه " CVE-2020-11651 "، در کلاس Clear-Funcs که به درستی method calls ها را اعتبارسنجی نمی‌کند قرار داشته و به مهاجمان اجازه می‌دهد تا توکن‌های کاربر را بازیابی کنند.

آسیب‌پذیری دیگر شناسه " CVE-2020-11652 " به آن اختصاص داده شده است، کلاس ClearFuncs به دلیل پاکسازی نامناسب، دسترسی به برخی روش‌ها را امکان پذیر می‌کند و همین امر موجب دسترسی دایرکتوری دلخواه به کاربران تصدیق هویت شده می‌شود.

طبق بررسی‌های انجام شده توسط تیم F-Secure، بیش از 6,000 نمونه از این سرویس در معرض اینترنت عمومی قرار گرفته است.

با گزارش آسیب‌پذیری‌های مذکور به SaltStack، اکنون نسخه 3000.2. با وصله آسیب پذیری‌های ذکر شده در دسترس کاربران قرار گرفته است و توصیه می‌شود آن را بروزرسانی نمایند.

منبع خبر :

https://gbhackers.com/saltstack-salt/

Scan Link

کشف نقص بحرانی در سه افزونه‌ی e-Learning محبوب وردپرس

محققان امنیتی در خصوص آسیب‌پذیری جدیدِ کشف شده در برخی از افزونه‌های محبوب سیستم‌های مدیریت آموزش آنلاین (LMS) به کاربران هشدار دادند، سازمان‌ها و دانشگاه‌های بسیاری جهت برگزاری دوره‌های آموزش آنلاین از طریق وب سایت‌های مبتنی بر وردپرس، از این سیستم‌ها استفاده می‌کنند. به گفته‌ی تیم تحقیقاتی Check Point سه افزونه[1] وردپرس LearnPress, LearnDash و LifterLMS دارای نقص امنیتی می‌باشند به طوری که به دانشجویان و همچنین کاربران غیرمجاز اجازه می‌دهند تا اطلاعات شخصی کاربران ثبت شده را به سرقت برده و حتی به امتیاز و سطح دسترسی معلمان نیز دست یابند.

Omri Herscovici که یکی از محققان Check Point می‌باشد اذعان داشت: "به دلیل شیوع ویروس کرونا، ناچار به یادگیری از راه دور و از طریق فضای مجازی هستیم و از طرفی نیز آسیب‌پذیری‌های کشف شده به دانشجویان و حتی به کاربران غیرمجاز اجازه می‌دهد تا اطلاعات حساسی را بدست آورده و یا کنترل پلتفرم‌های LMS را به دست گیرند."

سه سیستم LMS نام برده، حدوداً بر روی 100,000 پلتفرم آموزشی دانشگاه‌های مختلف از جمله دانشگاه‌های فلوریدا، میشیگان و واشنگتن نصب شده‌اند و LearnPress و LifterLMS نیز از زمان انتشارشان به تنهایی بیش از 1.6 میلیون بار دانلود شده‌اند.

LMS از طریق اپلیکیشن‌های مختلف، امر یادگیری آنلاین را برای کاربران تسهیل بخشیده و از این طریق مؤسسات آموزشی می‌توانند برنامه‌های درسی مختص خود را ایجاد کنند، آن‌ها را به اشتراک بگذارند، دانش‌آموزان را ثبت‌نام و آن‌ها را طریق برگزاری آزمون‌های مختلف ارزیابی کنند، افزونه‌های کاربردی LearnDash ، LearnPress و LifterLMS نیز با تطبیق هر سایت وردپرس با یک LMS کارآمد، توانسته‌اند این امر را آسان نمایند.

```
function learn_press_accept_become_a_teacher() {
  $action  = ! empty( $_REQUEST['action'] ) ? $_REQUEST['action'] : '';
  $user_id = ! empty( $_REQUEST['user_id'] ) ? $_REQUEST['user_id'] : '';
  if ( ! $action || ! $user_id || ( $action != 'accept-to-be-teacher' ) ) {
    return;
  }

  if ( ! learn_press_user_maybe_is_a_teacher( $user_id ) ) {
    $be_teacher = new WP_User( $user_id );
    $be_teacher->set_role( LP_TEACHER_ROLE );
    delete_transient( 'learn_press_become_teacher_sent_' . $user_id );
    do_action( 'learn_press_user_become_a_teacher', $user_id );
    $redirect = add_query_arg( 'become-a-teacher-accepted', 'yes' );
    $redirect = remove_query_arg( 'action', $redirect );
    wp_redirect( $redirect );
  }
}
add_action( 'plugins_loaded', 'learn_press_accept_become_a_teacher' );
```

نقص موجود در افزونه‌ی LearnPress، قادر به انجام حمله‌ی تزریق کد SQL (با شناسه‌ی CVE-2020-6010) و افزایش سطح دسترسی کاربر به سطح معلم (با شناسه‌ی CVE-2020-6011) می‌باشد.

محققان اظهار داشتند که:" کد مذکور، مجوزهای دسترسی را برای کاربران مختلف بررسی نخواهد کرد، بنابراین به هر دانش‌آموزی مجوز انجام هر کاری را خواهد داد."

به همین ترتیب آسیب‌پذیری موجود در افزونه‌ی LearnDash (با شناسه‌ی CVE-2020-6009) نیز با استفاده از شبیه‌ساز سرویس مسیجِ PayPal's Instant Payment Notification(IPN)، کد SQL مخرب را تزریق کرده و زمینه را برای ثبت‌نام دوره‌های جعلی آماده خواهد کرد.

نقص موجود در افزونه‌ی LifterLMS (با شناسه‌ی CVE-2020-6008) نیز از ماهیت اپلیکیشن‌های PHP سوءاستفاده کرده و به مهاجم اجازه می‌دهد تا تنها با یک قطعه کد مخرب PHP، نام پروفایل خود را تغییر دهد (به عنوان مثال، دانشجویی که برای دوره‌ی خاصی ثبت‌نام کرده است).

در نهایت این نقص‌ها باعث می‌شود تا مهاجمان بتوانند اطلاعات شخصی کاربران (مانند: نام، ایمیل، نام‌کاربری، گذرواژه‌ها و غیره) را به سرقت برده و دانش آموزان نیز بتوانند نمرات را تغییر دهند، سوالات آزمون‌های مختلف و پاسخ‌های آن‌ها را از قبل بدست آورند و همچنین قادر خواهند بود که گواهی‌نامه‌ها را جعل کنند.

محققان هشدار دادند که این پلتفرم‌ها شامل درگاه پرداخت بوده و مهاجم می‌تواند بدون اطلاع کاربر از طریق آسیب‌پذیری‌های مذکور، از طرح‌های مالی سوءاستفاده کند.

به گفته‌ی Check Point Research این آسیب‌پذیری‌ها در ماه مارس سال 2020 کشف شدند و برای هر یک از سیستم‌های LMS نام برده، وصله‌های امنتی منتشر شده است و به کاربران توصیه شود حتماً از نسخه‌های آپدیت این افزونه‌ها استفاده کنند.

منبع خبر :

https://thehackernews.com/2020/04/wordpress-lms-plugins.html

Scan Link

[1] plugin

بروزرسانی امنیتی OpenSSL

بروزرسانی امنیتی برای نرم‌افزار OpenSSL منتشر شد!

این بروزرسانی، جهت رفع یک آسیب‌پذیری با شدت بالا و شناسه "CVE-2020-1967" در این نرم‌افزار منتشر شده است. نقص امنیتی مذکور می‌تواند به منظور حمله‌ی انکار سرویس(DoS) توسط مهاجمان مورد اکسپلویت قرار گیرد. این آسیب‌پذیری به عنوان یک "segmentation fault" در تابع SSL_check_chain تعریف شده است.

ممکن است سرور یا اپلیکیشن‌های کلاینت که تابع SSL_check_chain() را حین یا پس از یک 1.3TLS فراخوانی می‌کنند، به دلیل عدم دسترسی به اشاره‌گر NULL، با اختلال مواجه شوند که این اختلال هنگامی رخ می‌دهد که الگوریتمی نامعتبر و ناشناخته از طرف یک همتای مخرب دریافت شود و این امکان را فراهم آورد تا این آسیب‌پذیری به منظور یک حمله‌ی انکار سرویس اکسپلویت شود.

این آسیب‌پذیری نسخه‌های 1.1.1 d، 1.1.1 e و 1.1.1 f نرم افزار OpenSSL را تحت تأثیر قرار می‌دهد و با انتشار نسخه 1.1.1 g؛ این نقص وصله شده است.

آسیب‌پذیری ذکر شده، توسط Bernd Edlinger کشف و در هفتم ماه آوریل 2020 به OpenSSL گزارش داده شد. Matt Caswell و Benjamin Kaduk نیز آنالیزهای تکمیلی دیگری در این خصوص انجام داده‌اند.

قابل ذکر است که نسخه‌های قدیمی این نرم‌افزار از جمله OpenSSL 1.0.2 و OpenSSL 1.1.0 تحت تأثیر این آسیب‌پذیری قرار نخواهند گرفت، از طرفی نیز این نسخه‌ها دیگر پشتیبانی نمی‌شوند و مشمول بروزرسانی‌های امنیتی نیز نخواهند شد. به کاربران توصیه می‌شود هر چه سریع‌تر نرم‌افزار خود را به نسخه‌ی OpenSSL 1.1.1 ارتقاء دهند!

منبع خبر :

https://bit.ly/2Ai9QcB

Scan Link

آسیب‌پذیری Command Injection در نرم‌افزار IOS XE SD-WAN سیسکو

یک آسیب‌پذیری در رابط خط فرمان یا CLI (Command Line Interface) نرم‌افزار IOS XE SD-WAN سیسکو کشف شده است که می‌تواند به یک مهاجم احراز هویت شده محلی اجازه دهد تا دستورات دلخواه خود را تزریق کرده و با سطح دسترسی root آنها را اجرا نماید.

این آسیب‌پذیری با شناسه "CVE-2019-16011" و شدت بالا، ناشی از اعتبارسنجی ناکافی در ورودی است و مهاجم قادر است با تایید هویت در دستگاه و ارسال ورودی ساختگی و دستکاری شده به ابزار CLI، از آن سوء استفاده کند. برای دسترسی به این ابزار، مهاجم حتما باید احراز هویت شود و در نهایت پس از یک اکسپلویت موفق، می‌تواند دستورات دلخواه خود را با سطح دسترسی root اجرا کند.

محصولات زیر در صورت اجرای یک نسخه آسیب‌پذیر از نرم‌افزار IOS XE SD-WAN، تحت تاثیر این آسیب‌پذیری قرار می‌گیرند:

- Series Aggregation Services Routers 1000
- (Series Integrated Services Routers (ISRs) 1000
- Series ISRs 4000
- Cloud Services Router 1000V Series

سیسکو تایید کرده است که آسیب‌پذیری مذکور، روی محصولات زیر تاثیر نخواهد داشت:

- IOS Software
- IOS XE Software
- vBond, vEdge, vManage, and vSmart software

این شرکت بروزرسانی‌های نرم‌افزاری را جهت رفع آسیب‌پذیری مذکور منتشر کرده است:

Fixed Releases

Cisco IOS XE SD-WAN Major Releases	First Fixed Release for This Vulnerability
16.9	Migrate to a fixed release.
16.10	Migrate to a fixed release.
16.11	Migrate to a fixed release.
16.12	Cisco IOS XE 17.2.1r

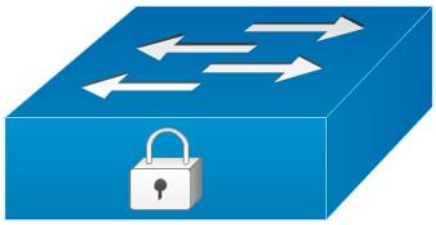
منبع خبر :

https://bit.ly/2YOBZSt

Scan Link

مقالات آموزشی

راهکارهاي امن‌سازی در سوئیچ‌های شبکه LAN



Secure switch

راهکارهاي امن‌سازی در سوئیچ‌های شبکه LAN

در سوییچ های لایه دسترسی یا Access امکاناتی امنیتی تعبیه شده است که می‌توان از آن ها در موارد لازم استفاده و کنترل شبکه داخلی خود را به صورت کامل در اختیار بگیرید، حتی با استفاده از برخی از این امکانات شما قادر به کنترل کردن دسترسی کاربران خود در شبکه نیز خواهید بود، شما می‌توانید از بروز بسیاری از حملات متداول در شبکه‌های LAN با پیاده‌سازی و استفاده درست از همین امکانات امنیتی پیشگیری کنید، برخی از مکانیزم‌های امنیتی که در سوئیچ‌ها تعبیه شده‌اند به شرح زیر می‌باشند :

- **Port Security یا امنیت پـــورت در سطح سوئیچ:** با استفاده از این قابلیـــت در سوییچ‌ها می‌توان تعریف کرد که صرفاً به ترافیکی که از یک آدرس مشخص MAC ایجاد شده است پاسخگو باشد. در این مکانیزم می‌توان برای سوئیچ آدرس‌های MAC معتبر را معرفی کرده تا فقط به آن‌ها سرویس‌دهی کند. روش‌های مختلفی برای معرفی آدرس‌های MAC به سوئیچ وجود دارد که به صورت دستی و همچنین به‌صورت خودکار انجـــام می‌شود. با پیاده‌سازی این مکانیزم امنیتی هیچ کامپیوتر عادی که به پورت‌های شبکه شما متصل می‌شود قادر به استفاده از منابع شبکه نخواهد بود، نوع برخورد با پورت‌های متخلف نیز در این مکانیزم امنیتی قابل تعیین است.
- **استفاده از قابلیت 802.1x (دات وان ایکس):** یکي از مکانیزم‌هاي امنیتي بسیار مناسب احراز هویت کاربران در لایه Access با استفـــــاده از روش ترکیبي AAA Authentication و Port Security مي‌باشد. با فعال سازي 802.1x پورت سوئیچ تا زماني که کاربر توسط آن احراز هویت نگردد، مجوز عبور هیچ‌گونه ترافیکي را از پورت مورد نظر نخواهد داد. معمولاً بـــــرای راه اندازی این سرویس از نرم‌افزارهایـــــا سرویس‌های اکانتینـــــگی مانند Cisco ACSو در نسخه‌های جدید این نرم‌افزارISE استفاده می‌شود.
- **DHCP Snooping یا جستجوگر:** یکی از حملاتی که در شبکه و بر روی سوئیچ‌ها انجام می‌شود به نام DHCP Spoofing یا جعل DHCP معروف

است که در آن هکر کامپیوتر خود را به عنوان DHCP سرور معتبر در شبکه معرفی می‌کند و با این روش می‌تواند آدرس DNS و Gateway کلاینت‌ها را آدرس مد نظر خود قرار دهد و ترافیک عبوری از این آدرس‌ها را شنود کند. با استفاده از قابلیت DHCP Snooping سوئیچ‌های موجود در شبکه صرفاً به DHCP سروری اجازه فعالیت می‌دهند که برای آن‌ها به عنوان سرور معتبر در نظر گرفته شده است و به سایر DHCP سرورها اجازه فعالیت نمی‌دهند. به این نوع فعالیت غیرمجاز DHCP ها در شبکه Rogue DHCP نیز می‌گویند.

- **IP Source Guard:** يكي ديگر از رايج‌ترين حمله‌ها جعل نمودن آدرس IP مي‌باشد. نفوذگر مي‌تواند از آدرس‌هاي جعلي كاربران ديگر و يا آدرس‌هاي موجود در شبكه استفاده نمايد. اين نوع حملات معمولاً براي حملات Denial-of-Service مورد استفاده قرار مي‌گيرند. با استفاده از اين مكانيزم، روترها و تجهيزات لايه 3 مي‌توانند با استفاده از برخي تست‌هاي ساده آدرس‌هاي IP جعلي را شناسايي نمايند. اين مكانيزم امنيتي به همراه مكانيزم DHCP Snooping و به همكاري سرويس DHCP در شبكه كار مي‌كند.
- **Dynamic ARP Inspection:** پروتكل ARP با ديد امنيتي طراحي و ايجاد نشده است و مي‌توان آن را با استفاده از حمله‌اي به نام ARP Spoofing يا ARP Cache Poisoning مورد حمله قرار داد و از آن سوء استفاده كرد. با استفاده از قابليت Dynamic ARP Inspection امكان بروز حملاتي از اين قبيل وجود نخواهد داشت، در ARP Spoofing هكر مي‌تواند خود را در وسط مسير تبادل اطلاعات قرار داده و خود را با استفاده از جعل ARP به عنوان يكي از طرفين ارتباط معرفي كند.
- **امن‌سازي عمليات STP:** به منظور جلوگيري از قرار دادن بسته‌هاي STP bridge protocol(BPD) درون شبكه توسط حمله‌كننده، لازم است قابليت BPDU Guard درون سوئيچ‌ها فعال گردد تا در صورت دريافت بسته BPDU مشكوك پورت سوئيچ به صورت اتوماتيك غيرفعال گردد.

علاوه بر امكانات امنيتي ذكر شده فوق، موارد امنيتي ديگري نيز وجود دارند كه در جلوگيري از دسترسي غيرمجاز به تجهيزات و شبكه داخلي سازمان بسيار مفيد مي‌باشند. اين موارد به شرح ذيل است:

- **Enable secret password:** استفاده از enable secret به جاي enable password ، در حالت enable password رمز عبور Privileged Mode شما به صورت Clear text نمايش داده مي‌شود اما اگر آن را به حالت Enable Secret در بياوريد با استفاده از الگوريتم Hashing به نام MD5 اين رمز عبور به‌صورت رمزنگاري شده نگهداري و نمايش داده مي‌شود.
- **service password-encryption:** با فعال نمودن اين سرويس تمامي password هاي ذخيره شده بر روي سوئيچ به صورت رمزگذاري شده ذخيره مي‌گردد.
- **امن سازي رابط تحت وب:** بسياري از مديران شبكه از دستورات سوئيچ براي مديريت شبكه استفاده مي‌نمايند. در اين حالت بايد اينترفيس تحت وب سوئيچ با دستور no ip http server غيرفعال گردد. زيرا لزومي ندارد زمانيكه شما از يک سرويس استفاده نمي‌كنيد آن سرويس فعال باشد. به اين فرآيند Switch Hardening نيز مي‌گويند.
- **امن‌سازي پورت console سوئيچ :** به منظور افزايش امنيت بهتر است Authentication بر روي تمامي پورت‌هاي كنسول سوئيچ‌ها فعال گردد.
- **استفاده از SSH:** استفاده از telnet آسان مي‌باشد ولي به دليل عدم رمزگذاري شدن اطلاعات ارتباط ناامن بوده و امكان استراق سمع username و password وجود دارد. در شرايطي كه امكان برقراري ارتباط از طريق SSH مي‌باشد، بهتر است كه از اين پروتكل استفاده شود.
- **كنترل دسترسي به تجهيزات با استفاده از SNMP:** به منظور جلوگيري از دسترسي غيرمجاز به تجهيزات با استفاده از SNMP بايد دسترسي Read و Write توسط اين پروتكل تنها به تعداد معدودي آدرس IP مشخص محدود گردد.

اخبار کوتاه

استفاده هکرها از وب‌سایت جعلی NHS برای انتشار بدافزار

متخصصان موسسه امنیتی IBM X-Force از حملات سایبری جدیدی خبر داده‌اند که در آن هکرها ایمیلی را به قربانیان خود ارسال کرده و مدعی نفوذ کرونا ویروس به کشور می‌شوند. در این ایمیل فایل‌هایی قرار دارد که ظاهرا حاوی اسناد راهنما در مورد ویروس کرونا است اما در واقع آلوده بوده و به محض دانلود شروع به نصب بدافزار Emotet می‌کند. این بدافزار نه تنها اجازه سرقت اطلاعات مهم کاربر را به هکر می‌دهد بلکه امکان انتقال فایل‌های خطرناک از جمله باج‌افزار را به سیستم قربانی فراهم می‌سازد.

کشف ۴۰۰۰ اپلیکیشن اندرویدی ناامن مبتنی بر پلتفرم Firebase

پلتفرم Firebase که به گوگل تعلق دارد از محبوبیت زیادی نزد توسعه دهندگان برای توسعه اپلیکیشن برخوردار است. حالا محققان امنیتی موسسه Comparitech از درز اطلاعات بالغ بر 4 هزار اپلیکیشن اندرویدی خبر داده‌اند و این اتفاق ظاهرا به خاطر پیکربندی نادرست در دیتابیس Firebase رخ داده است.

طبق آمارها حدود سی درصد از تمامی اپلیکیشن‌های گوگل پلی استور از Firebase استفاده می‌کنند و از تمامی اپلیکیشن‌های اندرویدی که از این پلتفرم برای ذخیره‌سازی دیتای خود کمک می‌گیرند، 4.8 درصدشان ایمن نیستند. این اپ‌ها اجازه دسترسی دیگران به اطلاعات کاربرانشان و ویرایش آنها را میسر می‌کنند.

بازی‌ها و اپلیکیشن‌های آموزشی ظاهرا 40 درصد از اپ‌های ناامنی را تشکیل می‌دهند که اطلاعات کاربران خود را در معرض دسترسی دیگران قرار داده‌اند. به لطف این آسیب‌پذیری آدرس ایمیل، نام کاربری، پسورد، شماره موبایل، دیتای جی پی اس، آدرس سکونت و بسیاری موارد دیگر بدون احراز هویت قابل دانلود خواهند بود.

تمامی این اتفاقات بر اهمیت انتخاب پسوردهای متفاوت برای لاگین به وبسایت‌ها یا اپ‌های مختلف صحه می‌گذارند چراکه اگر دیتای مربوط به یکی از اپ‌های مورد استفاده شما در اختیار هکرها قرار بگیرند آنها می‌توانند از همان پسورد برای دسترسی به دیگر حساب‌های شخصی شما نیز استفاده نمایند.

امنیت کاربر رایانه

مهندسی اجتماعی و سرقت هویت

همانطور که در بولتن شماره 19 نیز گفته شد، مهندسی اجتماعی روشی تاثیرگذار در ترغیب افراد، نسبت به فاش نمودن اطلاعات حساس آن‌ها می‌باشد که به منظور انجام اعمال خرابکارانه توسط مهاجمان به‌کار گرفته می‌شود. نفوذگران همواره به‌دنبال راه‌های جدید جهت کسب اطلاعات می‌باشند؛ آن‌ها از محیطی که قصد نفوذ به آن را دارند و از افرادی که در حلقه امنیتی آن محیط کار می‌کنند و همچنین از خطاهای سهوی منشی‌ها و هلپ‌دسک‌ها تا حد ممکن مطمئن سوء استفاده می‌کنند.

✓ حال با توجه به اهمیت این موضوع، در این شماره از بولتن خبری و در ادامه‌ی فصل " مهندسی اجتماعی و سرقت هویت " به بیان هشدارها و چک لیست‌های امنیتی در این زمینه می‌پردازیم.

با ما همراه باشید ...

چگونه متوجه شوید که قربانی سرقت هویت شده اید؟

اخطارهایی از شرکت های خدماتی مانند آب، تلفن و غیره مبنی بر عدم پرداخت قبوض به دست شما می رسد

قبض ها، فاکتورها و رسیدهای مربوط به **کالا** و خدماتی را دریافت می کنید که شما آن ها را سفارش نداده اید

برای مدت طولانی اطلاعات کارت اعتباری وصورت حساب های بانکی خود را دریافت نمی کنید

متوجه می شوید که برخی از ایمیل های شما ناپدید می شوند

درخواست وام شما به دلیل سوابق بدتان رد می شود، در حالی که سوابق شما خوب است

چگونه متوجه شوید که قربانی سرقت هویت شده اید؟

در کارت اعتباری یا صورت حساب های بانکی خود نقایصی را شناسایی می کنید

مدارک مهم مانند گذرنامه یا گواهینامه رانندگی را گم می کنید

در مورد یک آپارتمان که هرگز اجاره نکرده اید، خانه ای که هرگز خریداری نکرده اید، و یا کاری که شما هرگز انجام نداده اید، ایمیل دریافت کنید

درخواست های شما برای مزایای اجتماعی رد می شود

اطلاعات کارت اعتباری جدید، مربوط به یک حساب بانکی جدید دریافت می کنید

در صورت سرقت هویت چه کارهایی باید انجام داد؟

1. با شرکت یا آژانس های اعتباری کارت های خود تماس بگیرید
2. درباره فعالیت هایی که اخیرا با کارت های اعتباری شما انجام شده است ،اطلاع کسب نمایید
3. رمزهای عبور حساب های اینترنتی خود را تغییر دهید
4. حساب هایی را که گمان می کنید مورد سوء استفاده قرار گرفته اند ببندید

پلیس فتا مرکز شکایات جرائم سایبری

چنانچه قربانی سرقت هویت یا سایر جرایم سایبری شدید می توانید به سایت پلیس فتا بخش ارتباطات مردمی مراجعه کرده و اطلاعات لازم را وارد نمایید، به این ترتیب شکایت شما ثبت شده و پلیس فتا در اسرع وقت با شما جهت پیگیری پرونده تماس خواهد گرفت

https://www.cyberpolice.ir/page/20911

https://www.cyberpolice.ir/page/20911

سوء استفاده از سرقت هویت

1. با مراجعه به اداره، بانک یا هر سازمان دیگری که ممکن است در این مسئله درگیر باشد، روند را اغاز کنید
شکایات رسمی را دراداره پلیس ثبت نمایید

2. شکایت خود را در پلیس فتا ثبت نمایید اطلاعات خود را در سایت فتا دقیق وارد کرده و نوع سرقت هویت و سوء استفاده ای که شده را جهت پیگیری ثبت نمایید

3. یک کپی از شکایت را از اداره پلیس دریافت کرده و به سازمان هایی که گزارش سرقت هویت را به آن ها داده اید، ارائه دهید

4. به طور منظم از روند تحقیق اطلاع یابید، تا اطمینان حاصل کنید که پرونده به درستی مورد رسیدگی قرار گرفته است

مخفی کردن آی پی با استفاده از ابزار Quick Hide IP

- Quick Hide IP هویت اینترنتی شما را مخفی می کند و می توانید از اینترنت استفاده کنید بدون اینکه مکان و IPشما مشخص باشد
- این ابزار ترافیک اینترنت را از طریق پراکسی های ناشناس تغییر می دهد
- هنگامی که از این ابزار استفاده می کنید، وب سایت هایی را که بازدید می کنید به جای دیدن آدرس آی پی شما ، آدرس آی پی پراکسی سرورو را خواهند دید

ابزار های مخفی کردن آدرس IP

UltraSurf
http://www.ultrareach.com

Hide IP NG
http://www.hide-ip-soft.com

Hide My IP
http://www.hide-my-ip.com

TOR
http://www.torproject.org

IP Hider
http://www.iphider.org

Anonymizer Universal
http://www.anonymizer.com

Anti Tracks
http://www.giantmatrix.com

Hide The IP
http://www.hide-the-ip.com

خلاصه فصل

- سرقت هویت فرآیند استفاده از اطلاعات شخصی دیگران ،برای استفاده های شخصی هکر است
- مجرمان از طریق زباله گردی به دنبال صورتحساب یا کاغذ دیگری که اطلاعات شخصی روی آن باشد میگردند
- مجرمان با قربانی سرقت هویت تماس گرفته و با معرفی خود از طرف یک سازمان دولتی، از قربانی می خواهند اطلاعات شخصی خود را اعلام کند
- سیستم عامل کامپیوتر و برنامه های آن را به روز نگه دارید
- به ایمیل های ناخواسته که اطلاعات شخصی شما را درخواست می کنند پاسخ ندهید
- از رمز های عبور قوی برای حساب های مالی خود استفاده کنید
- به طور منظم گزارش های صورت حساب بانکی / کارت اعتباری خود را بررسی کنید

چک لیست حفاظت در مقابل سرقت هویت

- هرگز اطلاعات شخصی و اطلاعات حساب بانکی خود را در تلفن بازگو نکنید - مگرزمانی که شما آغاز کننده تماس تلفنی باشید
- کارت ها، گذرنامه، گواهینامه ها و دیگر اطلاعات شخصی ارزشمند خود را پنهان و در جای قفل دار نگه داری کنید
- کاغذهایی که حاوی اطلاعات شخصی شما هستند را ریز ریز کنید و دور بریزید و آن ها را تنها با مچاله کردن دور نیندازید
- اگر با شما تماس گرفته شد و خود را نماینده قانونی یک سازمان و غیره معرفی کردند حتما از صحت این مسئله اطمینان حاصل کنید
- فقط کارت های اعتباری ضروری را با خود حمل کنید
- مرتباً گزارش های اعتباری خود را مرور و بررسی کنید
- کارت های اعتباری خود را در کیف پول حمل نکنید
- به درخواست های ایمیل های ناخواسته برای اطلاعات شخصی پاسخ ندهید

چک لیست حفاظت در مقابل سرقت هویت

- اطلاعات شخصی را از طریق تلفن ارسال نکنید
- به طور منظم، گزارشات بانک / کارت اعتباری را بررسی کنید
- کارت های اعتباری خراب و چک های بدون استفاده را از بین ببرید
- هیچ اطلاعات مالی را در سیستم ذخیره نکنید و از کلمات عبور قوی برای تمام حساب های مالی استفاده کنید
- قبض های تلفن خود را برای پیدا کردن شماره هایی که شما با آن ها تماس نگرفته اید بررسی کنید
- قبل از کلیک روی چیزی آن را بخوانید، پیشنهادات اعتباری پیش تأیید شده را غیر فعال کنید، و سیاستهای حفظ حریم خصوصی وبسایت را مطالعه کنید
- سیستم عامل کامپیوتر و برنامه های دیگر را به روز نگه دارید
- آنتی ویروس نصب کنید و مرتب آن را به روز کنید

چک لیست حفاظت در مقابل سرقت هویت

- فایروال را فعال کنید
- قبل از واردشدن به وب سایت،سیاست های امنیتی آن را چک کنید
- هنگام باز کردن پیوست های ایمیل، مراقب باشید
- همیشه سابقه مرورگر، لاگ های مربوط، و پوشه مربوط به بازدیدهای اخیر را پاک کنید
- هنگام انتقال اطلاعات حساس وب سایت های ایمن را بررسی کنید

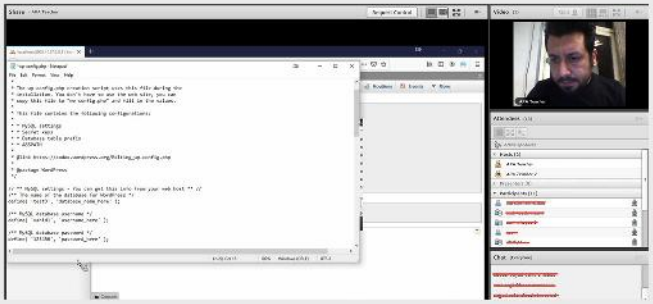
برگزاری وبینارها و دوره‌های آموزشی آنلاین

ثبت نام دوره‌های آموزشی آنلاین مرکز تخصصی آپا

مرکز تخصصی آپا دانشگاه رازی در راستای انجام رسالت خود در زمینه آگاهی‌رسانی و آموزش، اقدام به برگزاری دوره‌های آموزشی آنلاین با توجه به شرایط کنونی کشور نموده است. در این فصل از برگزاری دوره‌های آموزشی، ثبت‌نام سه دوره مقدماتی شبکه +Network، مقدماتی امنیت شبکه +Security و پیکربندی سوییچ‌های سیسکو CCNP Switch آغاز گردید. جزییات هر یک از دوره‌ها به صورت کامل در لینک https://evand.com/events/aparazi۹۹ ذکر شده است.

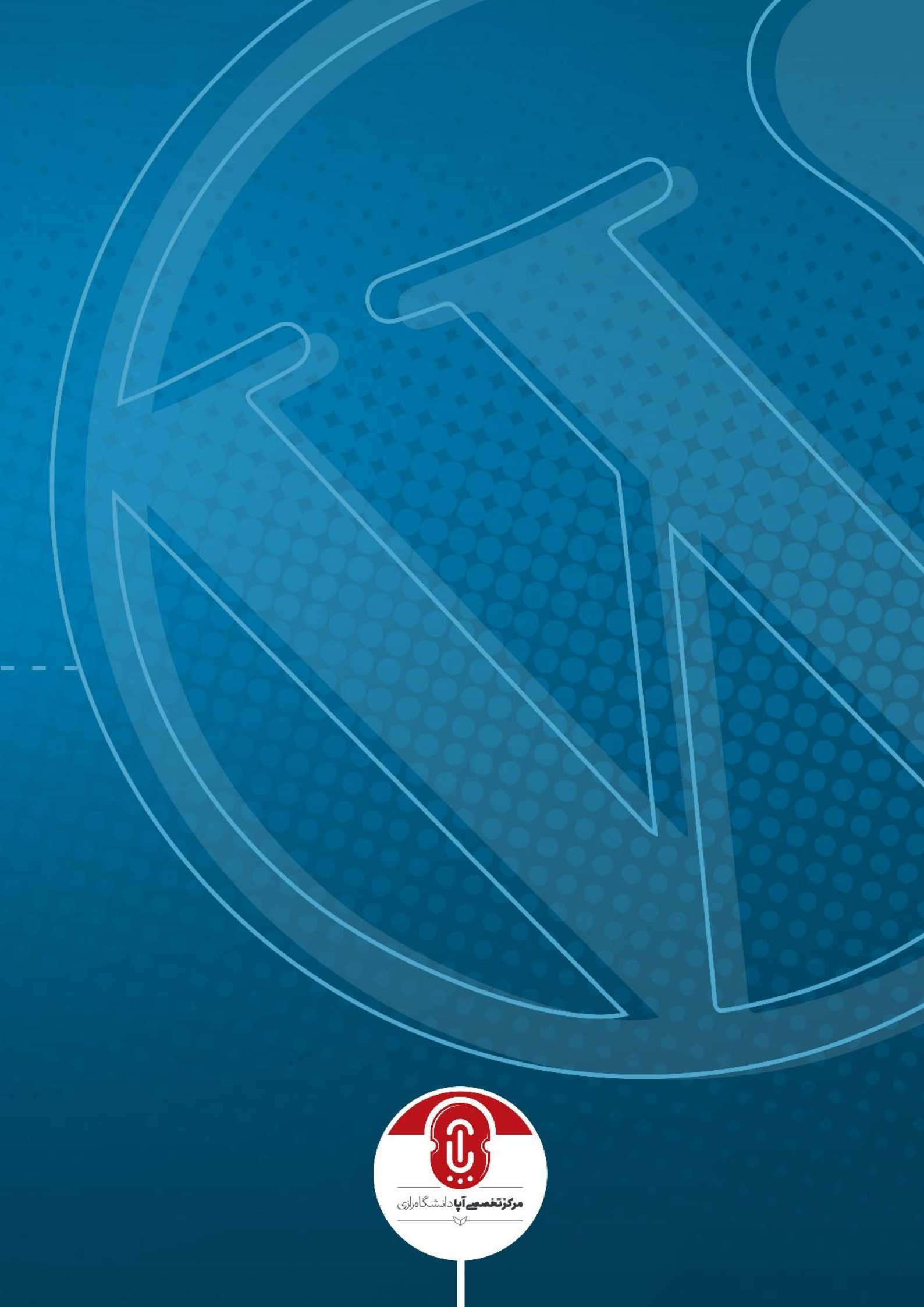
وبینار امنیت در وردپرس

برقراری و افزایش امنیت در وردپرس همواره یکی از چالشی‌ترین و مهمترین بحث‌ها در فضای وردپرس بوده است. وردپرس به دلیل محبوبیت زیادی که بین دیگر سیستم‌های مدیریت محتوا داشته و کاربران زیادی از آن استفاده می‌کنند، همیشه در معرض هک و نفوذ بیشتری قرار دارد. به همین دلیل توسط مرکز تخصصی آپا دانشگاه رازی یک وبینار رایگان تحت عنوان امنیت در Wordpress در مورخ ۵ اردیبهشت ۱۳۹۹ با حضور آنلاین دانشجویان و علاقمندان برگزار گردید. این وبینار توسط مهندس اشرف ارائه و برخی از رویکردهایی که باعث افزایش امنیت وردپرس می‌شود آموزش داده شد.



وبینار رایگان چالش‌های امنیت سایبری در دورکاری

با گسترش ویروس کرونا در سطح ایران و جهان و افزایش تهدید برای سلامتی افراد، دنیای کسب وکار در سه ماه اخیر دچار تغییرات زیادی شده است. این بیماری ترس گسترده‌ای را بین مردم ایجاد کرده و مشکلات عدیده‌ای برای اکثر کسب و کارها پدید آورده و منجر به تعطیلی یا کاهش جدی فعالیت بسیاری از سازمان‌ها و شرکت‌ها شده است. بسیاری از کارفرمایان به صورت داوطلبانه برای کاهش انتشار ویروس و کنترل بیماری و همچنین ادامه فعالیت‌های سازمانشان تصمیم به دورکاری گرفته‌اند. انجام وظایف در محیط خانه و به صورت دورکاری در کنار مزیت‌های بی‌شمار، دارای نقطه ضعف‌هایی نیز می‌باشد که آگاهی از آن‌ها می‌تواند کارکنان را در انجام هر چه بهتر وظایف یاری نماید. توجه به مسائل مرتبط با امنیت اطلاعات در شرایط دورکاری از جمله بزرگترین دغدغه‌های سازمان‌ها می‌باشد. از همین رو مرکز تخصصی آپا دانشگاه رازی در راستای انجام رسالت خویش در زمینه آگاهی‌رسانی، نکات و موارد امنیتی را جهت به حداقل رساندن تهدیدهای احتمالی در شرایط دورکاری، تصمیم به برگزاری وبیناری تحت عنوان چالش‌های امنیت سایبری در دورکاری در مورخ ۲۶ اردیبهشت ماه نموده، این وبینار با حضور آنلاین دانشجویان، پرسنل سازمان‌ها، شرکت‌ها و علاقمندان برگزار گردید.


مرکز تخصصی آپا دانشگاه رازی