بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره چهارم مهرماه ۱۳۹۷

رفع آسیب‌پذیری‌های حیاتی در تجهیزات سیسکو

در این شماره می‌خوانید:

فهرست

مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

صاحب امتیاز :
مرکز تخصصی آپا دانشگاه رازی

سردبیر :
سهیلا مرادی

همکاران این شماره :
پویان مسعودی‌نیا
سیده مرضیه حسینی
سهیلا مرادی
علی خزایی
سیده آرزو حسنی
آتوسا خدامرادی
محمد جلیلی
پروین زنگنه

صفحه آرایی و چاپ :
سهیلا مرادی
آژانس تبلیغاتی تمام خدمت باروک

آدرس :
کرمانشاه، بلوار طاق بستان، دانشگاه رازی، ساختمان کتابخانه مرکزی، طبقه دوم، مرکز تخصصی آپا

۰۸۳۳۴۲۷۳۳۹۰
cert.razi.ac.ir
apa@razi.ac.ir

فهرست

مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

صاحب امتیاز :
مرکز تخصصی آپا دانشگاه رازی

سردبیر :
سهیلا مرادی

همکاران این شماره :
پویان مسعودی‌نیا
سیده مرضیه حسینی
سهیلا مرادی
علی خزایی
سیده آرزو حسنی
آتوسا خدامرادی
محمد جلیلی
پروین زنگنه

صفحه آرایی و چاپ :
سهیلا مرادی
آژانس تبلیغاتی تمام خدمت باروک

آدرس :
کرمانشاه، بلوار طاق بستان، دانشگاه رازی، ساختمان کتابخانه مرکزی، طبقه دوم، مرکز تخصصی آپا

۰۸۳۳۴۲۷۳۳۹۰

cert.razi.ac.ir

apa@razi.ac.ir

اخبار امنیتی

هک واتس‌اپ تنها با پاسخ دادن به یک تماس تصویری!

اخبار امنیتی (گردآورنده: سهیلا مرادی)

آیا می‌دانید تنها با دریافت یک تماس تصویری در واتس‌اپ گوشی هوشمند شما می‌تواند هک شود؟!

یکی از محققان امنیتی شرکت Google Project Zero، به نام Natalie Silvanovich، یک آسیب‌پذیری حیاتی را در پیام‌رسان محبوب واتس‌اپ کشف نموده است که تنها از طریق یک تماس تصویری امکان دسترسی کامل به واتس‌اپ را از راه دور برای هکرها فراهم می‌سازد.

این آسیب‌پذیری یک باگ سرریز حافظه heap است، که با دریافت یک بسته RTP ساختگی و مخرب از طریق درخواست تماس تصویری، فعال شده و موجب ایجاد اختلال در برنامه واتس‌اپ و کرَش شدن آن می‌گردد.

از آنجا که این آسیب‌پذیری پیاده‌سازی RTP (Real-time Transport Protocol) را در واتس‌اپ تحت تأثیر قرار می‌دهد، بنابراین تمامی دستگاه‌های اندروید و iOS در معرض خطر هستند. تنها موردی که از این آسیب‌پذیری مصون است واتس‌اپ نسخه وب می‌باشد که برای تماس‌های تصویری از WebRTC استفاده می‌نماید.

Silvanovich کد اثبات مفهومی اکسپلویت این آسیب‌پذیری را به همراه دستورالعمل‌های حمله‌ی آن منتشر نمود.

Silvanovich فقط باگ موجود در حافظه را تحریک می‌کند، یکی دیگر از محققان شرکت Google Project Zero، به نام Tavis Ormandy، ادعا نموده که تنها پاسخ دادن به یک تماس از جانب مهاجم، می‌تواند برنامه واتس‌اپ را کاملاً در معرض خطر قرار دهد.

به عبارت دیگر هکرها برای اینکه بتوانند به حساب کاربری شما در واتس‌اپ دست یافته و مکالمات محرمانه شما را جاسوسی نمایند تنها به شماره تلفن شما نیاز دارند!

Silvanovich در ماه آگوست سال جاری آسیب‌پذیری مذکور را کشف، و آن را به تیم واتس‌اپ گزارش نموده است. تیم واتس‌اپ نیز با تأیید آسیب‌پذیری، در تاریخ ۲۸ سپتامبر این باگ را برای اندروید و در تاریخ ۳ اکتبر آن را برای آیفون برطرف نموده است.

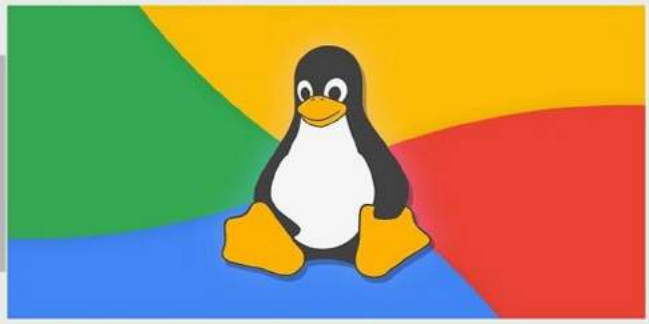
*بنابراین اگر هنوز واتس‌اپ خود را بروزرسانی ننموده‌اید، توصیه می‌گردد در اولین فرصت آن را هم در دستگاه‌های اندرویدی و هم در دستگاه‌های دارای سیستم‌عامل iOS آپدیت نمایید.

منبع خبر:

https://thehackernews.com/۰۹/۲۰۱۸/linux-kernel-exploit.html

کشف آسیب‌پذیری جدید در هسته لینوکس

اخبار امنیتی (گردآورنده: سهیلا مرادی)



یکی از محققان امنیتی شرکت Google Project Zero، جزئیات و کد اثبات مفهومی (PoC) یک آسیب‌پذیری بسیار حیاتی را که در هسته لینوکس، از نسخه ۳.۱۶ تا ۴.۱۸.۸

وجود دارد، منتشر نمود.

این آسیب‌پذیری با شناسه CVE-2018-17182، که توسط یک هکر کلاه سفید به نام Jann Horn کشف گردید، در واقع از وجود باگی در عدم اعتبارسنجی گَش در مدیریت حافظه لینوکس خبر می‌دهد که منجر به آسیب‌پذیری use-after-free می‌گردد. اگر این آسیب‌پذیری مورد سوءاستفاده قرار گیرد برای مهاجم امکان دسترسی به root سیستم هدف را فراهم می‌آورد.

آسیب‌پذیری use-after-free (UAF) نوعی از باگ‌های اختلال حافظه است که به منظور تغییر داده یا خراب نمودن آن در حافظه، می‌تواند توسط کاربران غیرمجاز مورد سوءاستفاده قرار گیرد، و آن‌ها را قادر به ایجاد حمله انکار سرویس (گَرش نمودن سیستم)، و یا افزایش حق دسترسی به منظور دستیابی به سطح دسترسی مدیر در سیستم نماید.

با اکسپلویت آسیب‌پذیری هسته لینوکس در کمتر از یک ساعت می‌توان به root سیستم دسترسی پیدا کرد!

Horn اظهار داشت که کد اثبات مفهومی وی به منظور اکسپلویت نمودن این آسیب‌پذیری در دسترس عموم قرار دارد.

Horn این آسیب‌پذیری را در ۱۲ سپتامبر به توسعه‌دهندگان هسته لینوکس گزارش نموده و تیم لینوکس نیز باگ مذکور را ظرف مدت دو روز در ساختار هسته لینوکس رفع نمود، آن‌گونه که Horn می‌گوید: "تیم لینوکس به نسبت سایر عرضه‌کنندگان نرم‌افزار بسیار سریع نسبت به رفع باگ اقدام نموده است."

آسیب‌پذیری هسته لینوکس در ۱۸ سپتامبر در لیست oss-security افشاء گردید و روز بعد در نسخه‌های ۴.۱۸.۹، ۴.۱۴.۷۱، ۴.۹.۱۲۸، ۴.۴.۱۵۷ و حتی در هسته نسخه ۳.۱۶.۵۸ وصله شد.

کاربران Debian و Ubuntu در مقابل این باگ آسیب‌پذیر هستند

Horn متذکر گشت که رفع باگ در هسته لینوکس بدین معنا نیست که سیستم‌های کاربران به صورت اتوماتیک وصله می‌شود، بنابراین کاربران کماکان در معرض خطر قرار دارند.

این محقق ضمن اظهار تأسف بیان داشت برخی از توزیع‌های عمده لینوکس مانند Debian و Ubuntu با وجود گذشت بیش از یک هفته از افشای این آسیب‌پذیری هنوز نسبت به، به روز رسانی هسته اقدام ننموده و کاربران خود را در معرض حملات احتمالی قرار داده‌اند.

این در حالی است که توزیع Fedora از لینوکس، در تاریخ ۲۲ سپتامبر وصله امنیتی را برای کاربران خود منتشر نموده است.

توسعه‌دهندگان اوبونتو در پاسخ به پست وبلاگ Horn اظهار داشتند که این شرکت احتمالاً در ۱ اکتبر ۲۰۱۸ وصله‌هایی را برای آسیب‌پذیری موجود در هسته لینوکس منتشر نماید!

منبع خبر:

https://thehackernews.com/۰۹/۲۰۱۸/linux-kernel-exploit.html

کشف جاسوس‌افزار قدرت‌مند اندروید و iOS که در ۴۵ کشور جهان گسترش یافته است

اخبار امنیتی (گردآورنده: آتوسا خدامرادی)

گزارش جدیدی که از Citizen Lab منتشر شده است از کشف جاسوس‌افزار خطرناک دیگری مختص اندروید و آیفون خبر می‌دهد که طی دو سال گذشته در ۴۵ کشور جهان گسترش یافته است.

Pegasus، محصول NSO Group بوده که به منظور هک از راه دور آیفون، اندروید و سایر دستگاه‌های قابل حمل طراحی شده است و بسیار قدرت‌مند می‌باشد. این جاسوس‌افزار به هکر اجازه می‌دهد که به طرز باور نکردنی به داده‌های قربانی دست پیدا کند، این در حالیست قربانی کاملاً از این موضوع بی‌اطلاع است! از جمله این داده‌ها می‌توان به پیام‌های متنی، موارد ذخیره شده در تقویم، پست‌های الکترونیکی، پیام‌های واتس‌اپ، موقعیت مکانی کاربر، میکروفون و دوربین دستگاه اشاره نمود. Pegasus، پیش از این برای هدف قرار دادن فعالان حقوق بشر و روزنامه‌نگاران از مکزیک تا امارات متحده عربی مورد استفاده قرار گرفته بود.

ماه گذشته، The Hacker News گزارش داد که این جاسوس‌افزار علیه یکی از کارمندان سازمان عفو بین الملل _که یکی از برجسته ترین سازمان های غیر حقوق بشری در جهان است_ استفاده شده است.

روز سه‌شنبه گزارشی از دانشگاه Citizen Lab تورنتو منتشر شد، این گزارش حاکی از آن بود که جاسوس‌افزار Pegasus به نسبت گذشته قربانیان بیشتری را هدف قرار داده است.

کشف ۳۶ عمل جاسوسی Pegasus در ۴۵ کشور

Citizen Lab ماه گذشته گزارش داد که تاکنون تعداد ۱۷۴ مورد، سوءاستفاده از افراد توسط جاسوس‌افزار NSO گزارش شده، اما اکنون ردپای Pegasus در بیش از ۴۵ کشور یافت شده است.

با توجه به گزارش، ۳۶ اپراتور Pegasus برای انجام عملیات نظارتی در ۴۵ کشور جهان مورد استفاده قرار گرفته است، و از این تعداد حداقل ۱۰ اپراتور فعالانه مشغول نظارت بر عملیات برون مرزی هستند.

همچنین بر اساس این گزارش، بعضی از مشتریان NSO به صورت کاملاً قانونی از Pegasus استفاده می‌کنند. حداقل ۶ کشور از این ۴۵ کشور از عملیات جاسوسی Pegasus آگاه بوده‌اند، به این معنا که آن‌ها قبلاً به جامعه سوءاستفاده از جاسوس‌افزار برای هدف قرار دادن جامعه مدنی پیوسته‌اند. این سوءاستفاده کنندگان از جاسوس‌افزار شامل بحرین، قزاقستان، مکزیک، مراکش، عربستان سعودی، و امارات متحده عربی می‌باشند.

لیست کشورهایی که مورد هدف Pegasus قرار گرفته‌اند شامل موارد زیر می‌باشد:

الجزایر، بحرین، بنگلادش، برزیل، کانادا، ساحل عاج، مصر، فرانسه، یونان، هند، عراق، اسرائیل، اردن، قزاقستان، کنیا، کویت، قرقیزستان، لتونی، لبنان، لیبی، مکزیک، مراکش، هلند، عمان، پاکستان، فلسطین، لهستان، قطر، روآندا، عربستان سعودی، سنگاپور، آفریقای جنوبی، سوئیس، تاجیکستان، تایلند، توگو، تونس، ترکیه، امارات متحده عربی، اوگاندا، بریتانیا، ایالات متحده، ازبکستان، یمن و زامبیا.

از آنجا که Citizen Lab، انتشار Pegasus را از طریق ایجاد اثر انگشت در زیرساخت Pegasus، و به وسیله

شناسایی آدرس‌های آی‌پی متعلق به سیستم‌های جاسوس‌افزار ردیابی می‌کند، ممکن است اشتباهاتی در گزارش ارائه شده وجود داشته باشد که دلیل آن استفاده گزینه‌های مورد هدف از VPN یا ارتباطات ماهواره‌ای می‌باشد.

Citizen Lab این اثرانگشت‌ها را مخفی نگه می‌دارد، اما اکنون دریافته است که آنها می‌توانند به وسیله اسکن کردن اینترنت شناسایی شوند.

پاسخ "NSO Group" سازنده جاسوس‌افزار

سخنگوی NSO Group با انتشار بیانیه‌ای عنوان کرد که این شرکت در تمامی موارد با توافق کامل با کشورها از جمله رعایت مقررات کنترل صادرات کار کرده است و هیچ‌گونه قانون‌شکنی صورت نگرفته است.

Shalev Hulio سخنگوی NSO Group در پاسخ به Citizen Lab گفت: "بر خلاف اظهارات شما، محصول ما مجوز دارد که به دولت‌ها و مراجع قانونی، به منظور رسیدگی به جرائم و جلوگیری از جرم و جنایت و تروریسم کمک کند. تجارت ما با قوانین کنترل صادرات انطباق کامل دارد."

کمیته اصول اخلاقی تجارت شرکت NSO (Business Ethics) که شامل کارشناسان خارجی از رشته‌های مختلف از جمله: حقوق و روابط خارجی می‌باشد، هر معامله‌ای را بررسی و سپس تصویب می‌کنند و حتی اگر یک مورد نامناسب استفاده شده باشد اجازه دارد توافقات را رد نموده و یا توافقات موجود را نادیده بگیرد.

گروه NSO همچنین اظهار داشت که در تحقیقات Citizen Lab اشتباهاتی وجود دارد، چرا که این شرکت در بسیاری از ۴۵ کشور یاد شده فروش محصول نداشته است!

منبع خبر:

https://thehackernews.com/۰۹/۲۰۱۸/android-ios-hacking-tool.html

نرم‌افزارهای مخرب در فروشگاه گوگل پلی برای سرقت اطلاعات بانکی کاربران!

اخبار امنیتی (گردآورنده: پویان مسعودی‌نیا)

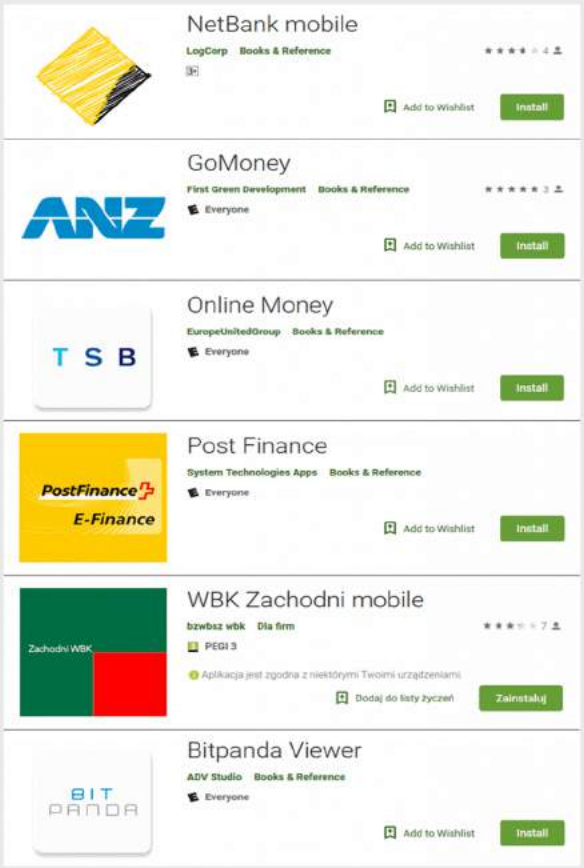
هکرها با آپلود کردن نرم‌افزارهای مالی جعلی در فروشگاه گوگل پلی در پی سرقت اطلاعات کارت‌های اعتباری کاربران و نیز اطلاعات ورود به حساب کاربری آنان به بانک یا سرویس‌های بانکی هستند!

این نرم‌افزارهای مخرب در ماه ژوئن ۲۰۱۸ در فروشگاه گوگل پلی آپلود شده و تا کنون هزاران بار بر روی تلفن‌های هوشمند دانلود و نصب گردیده‌اند.

نرم‌افزارهای مخرب، با استفاده از فرم‌های ساختگی و فریب دادن کاربران، اطلاعات کارت‌های بانکی و جزئیات تراکنش‌های اینترنتی بانکی آنان را جمع‌آوری می‌کنند. این نرم‌افزارها که با عناوین مختلف در گوگل پلی آپلود شده‌اند، توسط محققان امنیتی شرکت ESET شناسایی شده و مورد بررسی قرار گرفته‌اند.

انگیزه اصلی هکرها برای ساخت این‌گونه نرم افزارهای مخرب این است که اطلاعات حساس را از کاربران سرقت نمایند، و تا کنون نیز موفق شده‌اند شش بانک معتبر از کشورهای نیوزیلند، استرالیا، بریتانیا، سوئیس و لهستان را

تحت تاثیر قرار دهند که لیست برنامه‌های آن‌ها در زیر آورده شده است:



برنامه‌های جعلی چگونه عمل می‌کنند؟

عملکرد این برنامه‌ها بدین صورت است که یک فرم جعلی را به کاربر نشان داده و از وی درخواست می‌کنند اطلاعات کارت بانکی و یا اطلاعات ورود به حساب کاربری خود را وارد نماید، در صورت وارد نمودن اطلاعات خواسته شده، پیغام "Congratulations" یا "Thank you" به کاربر نشان داده خواهد شد. به محض وارد نمودن اطلاعات، کار نرم‌افزار به پایان رسیده و اطلاعات در اختیار هکرها قرار می‌گیرد.

شرکت ESET برنامه‌های جعلی را به گوگل گزارش نموده و این برنامه‌ها اکنون از گوگل پلی حذف شده‌اند.

به کاربران توصیه می‌شود که فوراً این برنامه‌های جعلی را از دستگاه‌های خود حذف نموده و اطلاعات ورود به حساب کاربری خود را تغییر دهند.

راهکارهای مصون ماندن از آسیب برنامه‌های جعلی و مخرب

- توجه دقیق به مجوزهای درخواست شده توسط برنامه‌ها هنگام نصب
- دانلود برنامه‌ها از منابع معتبر و قابل اطمینان
- بروز رسانی مداوم برنامه‌ها
- رمزگذاری دستگاه
- پشتیبان‌گیری مکرر از داده‌ها و اطلاعات مهم
- نصب آنتی‌ویروس و آنتی‌تروجان بر روی دستگاه

منبع خبر:
https://gbhackers.com/hackers-fake-apps-in-to-google-play/

مراقب باشید! گوشی آیفون شما می تواند توسط یک وب اکسپلویت از کار بیفتد

اخبار امنیتی (گردآورنده: سهیلا مرادی)

تنها چند خط کد می تواند گوشی آیفون یا آیپد شما را از کار انداخته و حتی عملکرد کامپیوتر مک شما را متوقف نماید!

یک محقق امنیتی به نام Sabri Haddouche، یک صفحه‌ی وب را جهت اثبات این مفهوم (PoC) نشان داده است، این صفحه حاوی اکسپلویتی است که از چند خط کد Html و CSS ساختگی استفاده می‌کند.

حتی فراتر از یک آسیب ساده، در صورت بازدید از این صفحه وب، کل هسته دستگاه تحت تأثیر قرار گرفته و موجب ریستارت شدن سیستم می‌گردد.

اکسپلویت اثبات مفهومی Haddouche، از یک ضعف در موتور WebKit اپل بهره می گیرد، که توسط تمام اپلیکیشن ها و مرورگرهای وب در حال اجرا بر روی سیستم عامل اپل مورد استفاده قرار می گیرد.

از آنجا که Webkit نمی‌توانست المان‌های متعدد، مانند تگ‌های "div" را داخل صفت backdrop-filter در CSS به درستی بارگذاری نماید، Haddouche یک صفحه وب ایجاد نمود که از تمام منابع دستگاه استفاده نموده و موجب خاموش و ریستارت شدن دستگاه می‌شد.

با مشاهده این ویدئو که توسط محقق نامبرده در یوتیوب به اشتراک گذاشته شده است می‌توانید جزئیات این حمله را در عمل ببینید.

تمامی مرورگرها مانند Microsoft Edge، Internet Explorer و سافاری در iOS، و همچنین سافاری و Mail در سیستم‌عامل مک در مقابل این حمله‌ی مبتنی بر CSS آسیب‌پذیر هستند، چرا که تمام این مرورگرها از موتور WebKit استفاده می‌کنند.

لازم به ذکر است که کاربران ویندوز و لینوکس تحت تأثیر این آسیب پذیری قرار نمی گیرند.

تیم هکر نیوز این حمله را بر روی مرورگرهای دیگر مانند کروم، سافاری و Edge (در MacBook Pro و iPhone X) نیز تست نمودند و دریافتند که هنوز هم بر روی آخرین نسخه هر دو سیستم‌عامل macOS و iOS کار می‌کند.

Haddouche اظهار داشت موضوع آسیب پذیری در Webkit را به اپل گزارش داده و احتمالاً شرکت در حال بررسی و تلاش برای رفع این آسیب پذیری در آینده است.

* بنابراین، به کاربران اپل توصیه می‌شود هنگام بازدید از هر وب‌سایتی که شامل کد یا لینک بوده و از طریق حساب کاربری فیسبوک و یا واتس‌اپ برای آن‌ها فرستاده شده است مراقب باشند.

منبع خبر:

https://thehackernews.com/۰۹/۲۰۱۸/iphone-crash-exploit.html

کشف مشکل امنیتی Zero-day توسط محققین که تمام نسخه‌های ویندوز را تحت تاثیر قرار می‌دهد

اخبار امنیتی (گردآورنده: علی خزایی)

یک محقق امنیتی، آسیب‌پذیری روز صفرم وصله نشده‌ای را در تمام نسخه‌های ویندوز شرکت مایکروسافت کشف کرده است. وی بعد از گذشت ۱۲۰ روز، و وصله نشدن این آسیب‌پذیری آن را منتشر نمود.

این مشکل امنیتی توسط آقای Lucas Leong از تیم تحقیقاتی Trend Micro Security منتشر شده است. آسیب‌پذیری روز صفرم در موتور پایگاه داده Microsoft jet قرار دارد و به مهاجم اجازه می‌دهد

کد مخرب را از راه دور بر روی هر رایانه‌ای با سیستم‌عامل ویندوز اجرا کند.

موتور پایگاه داده مایکروسافت (Joint Engine Technology) JET، موتور پایگاه داده یکپارچه در چندین محصول مایکروسافت، از جمله Microsoft Access و ویژوال بیسیک می‌باشد.

با توجه به توصیه‌های منتشر شده توسط Zero Day Initiative (ZDI)، این آسیب‌پذیری ناشی از مشکلی در مدیریت شاخص‌ها در موتور پایگاه داده JET است که اگر با موفقیت اکسپلویت شود، می‌تواند موجب نوشتن خارج از محدوده حافظه شده و در نهایت منجر به اجرای کد از راه دور گردد.

مهاجم باید کاربر هدف را برای باز کردن فایل پایگاه داده ویژه JET متقاعد کند تا از این آسیب‌پذیری به منظور اجرای راه دور کدهای مخرب بر روی رایانه ویندوزی استفاده نماید.

به گفته محققان ZDI، آسیب‌پذیری مذکور در تمام نسخه‌های ویندوز از جمله ویندوز ۱۰، ویندوز ۸.۱، ویندوز ۷ و ویندوز سرور نسخه ۲۰۰۸ تا ۲۰۱۶ وجود دارد.

ZDI این آسیب‌پذیری را در هشتم ماه مه به مایکروسافت گزارش نمود و غول تکنولوژی، این خطا را در چهاردهم ما مه تأیید کرد اما موفق به وصله کردن آن نشد و در یک مهلت ۱۲۰ روزه (٤ ماه) نتوانست به‌روزرسانی آن را منتشر نماید.

کد اکسپلویت این آسیب‌پذیری در صفحه GitHub Trend Micro نیز منتشر شده است.

مایکروسافت در حال کار بر روی وصله این آسیب‌پذیری است و از آنجایی که در ماه سپتامبر وصله آن عرضه نشده است، می‌توان در ماه اکتبر انتظار نسخه وصله شده را داشت.

Trend Micro به تمامی کاربرانی که از این آسیب‌پذیری صدمه دیده‌اند توصیه می‌کند که تا زمانی که مایکروسافت وصله مورد نظر را ارائه می‌کند، تعامل با برنامه را تنها به فایل‌های مورد اعتماد محدود نمایند.

منبع خبر:

https://thehackernews.com/۰۹/۲۰۱۸/windows-zero-day-vulnerability.html

حمله جدید Cold Boot بر روی کامپیوترهای مدرن

اخبار امنیتی (گردآورنده: سیده مرضیه حسینی)

محققان امنیتی حمله جدیدی کشف کردند که حتی دیسک‌های رمزگذاری شده در کامپیوترهای مدرن را نیز تحت تأثیر قرار می‌دهد!

این حمله می تواند رمزهای عبور، کلیدهای رمزنگاری و سایر اطلاعات حساس کاربر را در اختیار مهاجم قرار دهد.

این حمله، نوع جدیدی از حملات قدیمی و سنتی Cold Boot بوده که از حدود سال ۲۰۰۸ آغاز گشته و به هکرها اجازه می‌دهد تا اطلاعاتی که پس از خاموش شدن کامپیوتر، به طور موقت در حافظه (RAM) باقی می‌ماند را سرقت نمایند.

با این وجود، به منظور کاهش تأثیر حملات cold boot، برای اکثر کامپیوترهای مدرن تمهیدات امنیتی مؤثری توسط گروه TCG (Trusted Computing Group) در نظر گرفته شده است، که به منظور جلوگیری از خواندن داده، محتوای حافظه را زمانی که پاور دستگاه در حال راه‌اندازی مجدد است، بازنویسی می‌کند.

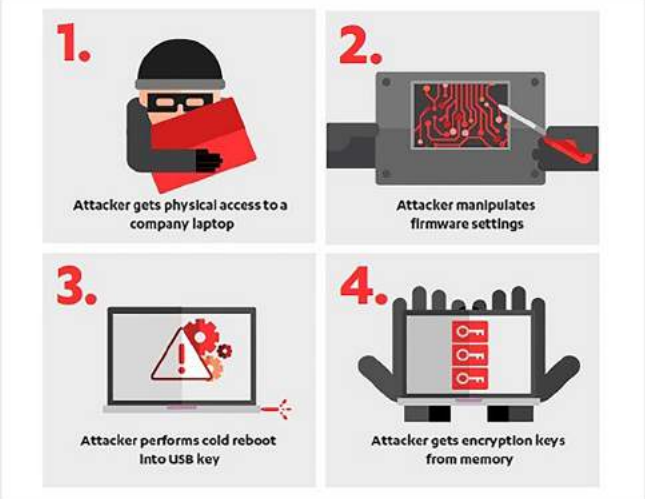
اکنون محققان شرکت امنیت سایبری فنلاند ملقب

به (F-Secure) ، با استفاده از دستکاری فیزیکی میان‌افزار کامپیوتر، روش جدیدی را برای غیرفعال کردن این معیار امنیتی بازنویسی شده کشف کردند، که به طور بالقوه مهاجمان را قادر به بازیابی اطلاعات حساس ذخیره شده در کامپیوتر بعد از راه‌اندازی مجدد می‌کند.

نکته جالب این است که محققان با استفاده از یک ابزار ساده توانستند حافظه غیرفرار را که حاوی تنظیمات است بازنویسی نموده، و همچنین آن را غیرفعال نمایند و یا قابلیت بوت شدن از روی دستگاه‌های خارجی را در آن فعال کنند.

البته ناگفته نماند که همانند حملات مرسوم گذشته Cold Boot، حمله‌ی جدید هم به منظور بازیابی داده‌های باقی مانده در حافظه‌ی دستگاه، نیازمند دسترسی فیزیکی به سیستم هدف می‌باشد.

چگونه کاربران مایکروسافت و اپل می‌توانند از حملات Cold Boot جلوگیری کنند؟



به گفته Olle و همکارش Pasi Saarinen، این تکنیک حمله تمام کامپیوترهای مدرن، از سیستم‌های ویندوزی گرفته تا مکینتاش را تحت تأثیر قرار می‌دهد، و نمی‌توان به سرعت و به سادگی آن را وصله نمود.

این دو محقق، که این روزها در کنفرانس‌های امنیتی یافته‌هایشان را ارائه نموده‌اند، اظهار داشتند که پیش از این یافته‌های خود را با مایکروسافت، اینتل و اپل به اشتراک گذاشته و در مورد استراتژی‌های کاهش حمله به آن‌ها کمک نموده‌اند.

شرکت مایکروسافت در واکنش به یافته‌های F-Secure، تمهیدات امنیتی خود را بر روی Bitlocker آپدیت نمود، این در حالی است که به گفته شرکت اپل، دستگاه‌های مک این شرکت به منظور محافظت از کاربران در مقابل این حمله به تراشه Apple T۲ مجهز شده‌اند.

اما برای کامپیوترهای مک فاقد تراشه T۲، اپل به کاربران توصیه نمود تا یک رمز میان‌افزاری به منظور کمک به افزایش امنیت کامپیوترهای خود، تنظیم نمایند.

با توجه به اظهارات Duo محقق امنیتی فعال در این زمینه، هنگامی که مهاجم سیستمی را مورد هدف قرار می‌دهد، هیچ راه قابل اطمینانی برای مسدود نمودن یا جلوگیری از حمله cold boot وجود ندارد، اما پیشنهاد می‌شود که شرکت‌ها دستگاه‌های خود را به گونه‌ای پیکربندی کنند تا مهاجمان با استفاده از حملات cold boot، هیچ چیز ارزشمندی برای سرقت نیابند.

در عین حال، این محقق به کارشناسان فناوری اطلاعات توصیه می‌کند تمام کامپیوترهای سازمان را در حالت Hibernate قرار داده و یا خاموش کنند (در حالت sleep قرار ندهید) و کاربران را وادار نمایند تا هنگام ورود به سیستم ها و یا روشن نمودن آن‌ها BitLocker PIN آن‌ها را وارد نمایند.

البته با در نظر گرفتن تمهیدات امنیتی که در

بالا به آن‌ها اشاره شد مهاجمان باز هم می‌توانند یک حمله cold boot موفق را علیه کامپیوترهایی که به شیوه فوق پیکربندی شده‌اند انجام دهند، اما از آنجا که کلیدهای رمزگذاری هنگامی که سیستم در حالت hibernate و یا خاموش قرار دارد در حافظه ذخیره نمی‌گردند، بنابراین اطلاعات با ارزشی برای سرقت مهاجم وجود نخواهد داشت.

منبع خبر:

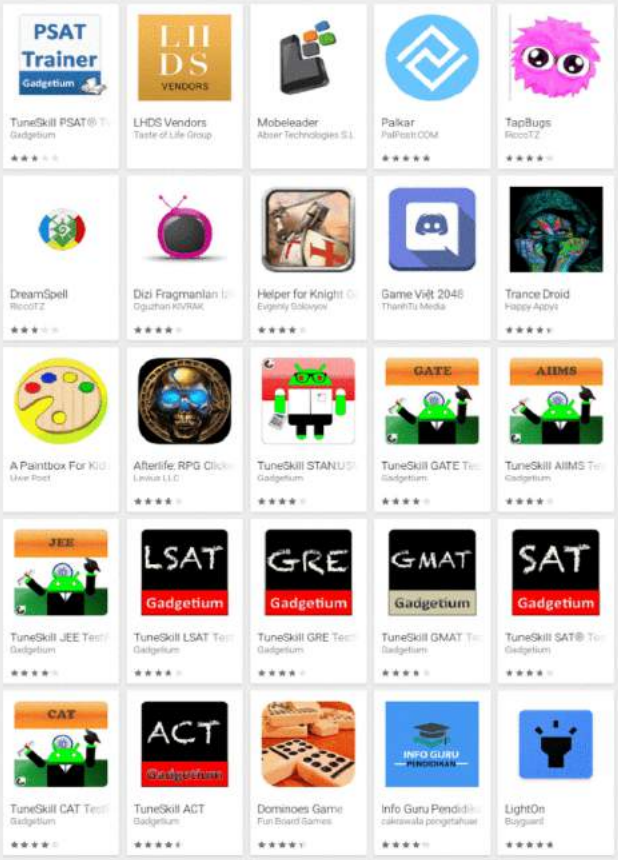
https://thehackernews.com/۰۹/۲۰۱۸/cold-boot-attack-encryption.html

کشف اپلیکیشن‌های حاوی اسکریپت استخراج ارز در گوگل پلی

اخبار امنیتی (گردآورنده: محمد جلیلی)

تولیدکنندگان بدافزار کماکان بدافزارهای حاوی اسکریپت‌های مخفی استخراج ارز دیجیتال را در گوگل پلی آپلود می‌کنند. مهاجمان این برنامه‌های مخرب را در قالب بازی‌ها، برنامه‌های کاربردی مانند چراغ قوه و برنامه‌های آموزشی آپلود می‌کنند، اما پشت پرده‌ی این برنامه‌ها اسکریپت‌هایی پنهان شده است که در قالب برنامه‌های مخرب به استخراج ارز دیجیتال می‌پردازد.

آزمایشگاه Sophos بیش از ۲۵ برنامه مخرب را مشخص نمود که حاوی اسکریپت‌های مخفی استخراج‌کننده ارز دیجیتال بوده و دستگاه قربانیان را به استخراج کننده ارز دیجیتال تبدیل می‌کند.



این برنامه‌های مخرب بیش از ۱۲۰،۰۰۰ بار از فروشگاه گوگل پلی دانلود شده‌اند. اسکریپت‌های مخفی شده در پسِ پرده‌ی این برنامه‌ها ارز monero را استخراج می‌کنند.

اسکریپت استخراج‌کننده، تنها چند خط کد است که می تواند به هر اپلیکیشنی که از مرورگر WebView به صورت داخلی استفاده می‌کند، اضافه شود. این برنامه‌های مخرب ابتدا جاوا اسکریپت را فعال نموده و سپس با استفاده از یک صفحه HTML در WebView، فرآیند استخراج ارز را آغاز می‌نمایند.

محققـان دریافتنـد کـه اکثـر اپلیکیشـن‌ها از اسکریپت‌های استخراج‌کننده coinhive (نوعی بدافزار کـه در صفحـات وب بـرای اسـتخراج ارز دیجیتـال مـورد اسـتفاده قـرار می‌گیـرد) اسـتفاده می‌کننـد، برخـی از آن‌هـا اسـکریپت‌ها را بـر روی سـرورهای خـود قـرار می‌دهنـد و برخـی دیگـر از XMRig (نوعی استخراج‌کننده) استفاده می‌کنند.

از آغـاز سـال ۲۰۱۸، تهدیـدات سـایبری از باج‌افـزار بـه سـمت حمـلات اسـتخراج ارز دیجیتـال سـوق یافتـه و مهاجمـان انـواع پورتال‌هـای وب، دسـتگاه‌های اندرویـدی و انـواع سـرورها هـدف قرار داده‌اند.

منبع خبر:

https://gbhackers.com/-۲۵malicious-apps-cryptomining-script/

اسـتفاده از دسـتگاه‌های USB و رسـانه‌های قابـل حمـل بـرای تزریـق اسـتخراج کننده ارز دیجیتال

اخبار امنیتی (گردآورنده: پروین زنگنه)

بـد نیسـت بدانیـد کـه مجرمـان سـایبری هنـوز از دسـتگاه‌های USB و رسـانه‌های قابل حمل برای انجام فعالیت‌هـای مخـرب و گسـترش بدافزارهـای اسـتخراج ارز، بـه منظـور اسـتخراج ارز، بـه ویـژه بیت‌کوین استفاده می‌کنند.

گزارش‌هـای اخیـر شـرکت کسپرسـکی نشـان می‌دهـد کـه حـدوداً از هـر چهـار کاربـر در سراسـر جهـان یـک نفـر توسـط دسـتگاه‌های USB و دیگـر رسـانه‌های قابـل حمـل تحـت تأثیـر یـک رخـداد سایبری محلی قرار می‌گیرد.

گرچـه امـروزه در دنیـای دیجیتـال از سـرویس‌های ابـری بـرای ذخیـره و نگهـداری داده‌هـا اسـتفاده می‌شـود امـا هنـوز هـم میلیون‌هـا دسـتگاه USB در سراسـر دنیـا در حـال تولید و توزیع می‌باشد.

آلـوده نمودن سیسـتم کاربران از طریق دسـتگاه‌های USB از سـال ۲۰۱۶ مـورد اسـتفاده قـرار گرفتـه و برخـی از قربانیـان، بیـش از یـک سـال درگیـر ایـن آلودگی بدافزاری بوده‌اند.

در ایـن میـان، آسـیا، آفریقـا و آمریـکای جنـوبی دچـار بیشـترین آسـیب‌دیدگی، و برخـی از آسـیب‌های سـنگین‌تر در اروپـا و آمریـکای شـمالی دیده شده است.

غیـر از بدافزارهـای اسـتخراج ارز، بدافزارهـای دیگـری نیـز وجـود دارنـد کـه از طریـق رسـانه‌های قابـل حمـل یـا USBهـا گسـترش یافتـه و شـامل خانواده تروجان‌های Windows LNK می‌باشد که یکی از تهدیدات سایبری مهم در سال ۲۰۱۶ بوده است.

بدافـزار Windows LNK از بدافزارهـای خانـواده ویندوز بـوده (بدافـزاری حـاوی لینک‌هـای مخـرب بـرای دانلـود فایل‌هـای آلـوده، و یـا حـاوی مسـیری بـرای اجـرای یـک فایـل اجـرایی مخـرب) کـه توسـط مهاجمـان بـرای از بیـن بـردن، مسـدود نمـودن، تغییـر یـا کـپی داده‌هـا و یـا بـرای ایجـاد اختـلال در عملکـرد دسـتگاه یـا شـبکه مـورد اسـتفاده قـرار می‌گیـرد و ایـن خـود یـکی از تهدیـدات بـزرگ مبتـنی بر USB در سال ۲۰۱۶ می‌باشد.

تروجـان WinLNK Runner کـه بـه عنـوان یـکی از تهدیدات مهم سـال ۲۰۱۷ شناخته شده بود، با ۲۲/۷ میلیـون بـار تلاش توانسـت حـدود ۹۰۰،۰۰۰ کاربر را آلوده نماید.

بـر اسـاس تحقیقـات صـورت گرفتـه در آزمایشـگاه

کسپرسکی، امسال این تعداد به ۲۳ میلیون افزایش یافته و بیش از ۷۰۰،۰۰۰ کاربر را تحت تأثیر قرار داده است.

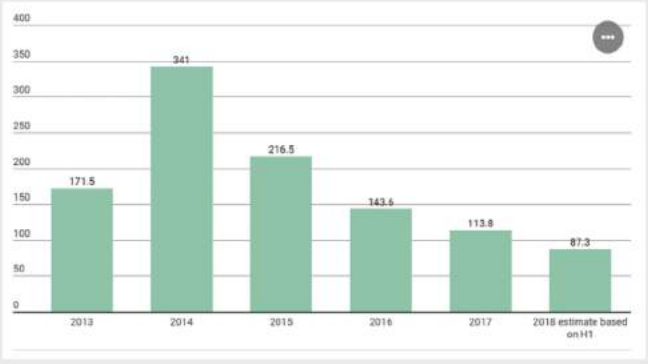
از نمونه‌های این بدافزار می‌توان به Stuxnet در سال ۲۰۱۰ اشاره نمود، که یکی از ده مورد بدافزار مخرب گسترش یافته از طریق رسانه قابل حمل می‌باشد.

فرآیند آلوده شدن به بدافزار مبتنی بر USB

آلودگی از طریق دستگاه‌های USB به عنوان یک تهدید محلی که سیستم کاربر را آلوده می‌کند، در نظر گرفته می‌شود.

به گفته آزمایشگاه کسپرسکی، تهدیدات محلی متفاوت از تهدیداتی هستند که کامپیوترها را از طریق اینترنت هدف قرار می‌دهند (تهدیدات اینترنتی) و بسیار نیز شایع هستند. تهدیدات محلی می‌توانند در یک برنامه اجرایی پنهان شده و از طریق یک برنامه مخرب رمزگذاری شده، عمل مخرب خود را انجام دهند.

در سال‌های ۲۰۱۳ تا ۲۰۱۸، حملات مبتنی بر دستگاه‌های USB به طور چشمگیری افزایش یافته است.



گروه‌های فعال در این زمینه، مانندگروه Equation، Regin، Flame و تیم Hacking اکسپلویت مذکور را به آسیب‌پذیری Windows LNK در ویندوز با شناسه CVE-2010-2568 ارتباط داده‌اند.

دستگاه‌های USB برای گسترش بدافزارهای استخراج‌کننده ارز غیرمعمول نیز مورد استفاده قرار می‌گیرند، بدین معنا که از طریق بدافزاری که به صورت مخفیانه از ظرفیت پردازنده کامپیوتر آلوده برای تولید ارز استفاده می‌کند، به سیستم هدف تزریق می‌شوند.

راهکارهای مقابله

راهکارهای زیر به تمامی کاربران دستگاه‌های USB توصیه می‌گردد.

۱- مراقب دستگاه‌هایی که به سیستم خود متصل می‌کنید باشید_ این دستگاه‌ها از کجا آمده‌اند؟

۲- هنگام خرید دستگاه‌های USB، محصولات دارای برند و شناخته شده را خریداری نمایید_ با این شیوه اطمینان خواهید داشت که حتی اگر دستگاه شما دچار مشکل شود داده‌های شما آسیب نخواهند دید.

۳- اطمینان حاصل کنید که اطلاعات شما در USB به صورت رمزنگاری شده ذخیره شده‌اند.

۴- به منظور اطمینان حاصل از عدم وجود بدافزار، یک راه‌حل امنیتی برای بررسی رسانه‌های قابل حمل قبل از اتصال به شبکه داشته باشید.

توصیه‌هایی برای صاحبان کسب و کار:

۱- استفاده از دستگاه‌های USB را مدیریت کنید، یعنی تعیین کنید که کدام دستگاه‌های USB، توسط چه کسی و برای چه چیزی می‌توانند مورد استفاده قرار گیرند.

۲- آموزش کارکنان در مورد شیوه‌های استفاده امن از دستگاه‌های USB، به ویژه اگر از دستگاه هم در محیط کار و هم برای کارهای شخصی در منزل نیز استفاده می‌کنند.

۳- USB را در معرض دید یا جای نامطمئن قرار ندهید.

منبع خبر:

https://gbhackers.com/beware-usb-devices-removable-media-are-being-used-to-inject-cryptocurrency-mining-malware/

آسیب پذیری

آسیب‌پذیری دور زدن فرآیند احراز هویت در مرکز معماری شبکه دیجیتال سیسکو

آسیب‌پذیری (گردآورنده: آتوسا خدامرادی)

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری Critical می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پذیری با شناسه CVE-2018-0448 در سرویس مدیریت هویت مربوط به مرکز معماری شبکه دیجیتال سیسکو (DNA) وجود داشته و به هکر احراز هویت نشده اجازه می‌دهد که فرآیند احراز هویت را دور زده و کنترل کامل توابع مدیریت هویت را به دست بگیرد.

آسیب‌پذیری یافت شده ناشی از اعمال محدودیت‌های امنیتی ناکافی در توابع مدیریتی حیاتی می‌باشد. هکر می‌تواند با استفاده از ارسال درخواست مدیریت هویت معتبر به سیستم در معرض خطر، این آسیب‌پذیری را اکسپلویت نماید. آسیب‌پذیری مذکور به هکر اجازه مشاهده و اصلاح غیر مجاز کاربران موجود در سیستم را می‌دهد، به عنوان مثال می‌تواند کاربران دیگری در سیستم ایجاد کند.

محصولات آسیب‌پذیر

تمام نرم‌افزارهای مرکز معماری شبکه دیجیتال سیسکو (DNA) که قبل از نسخه ۱.۱.۴ منتشر شده‌اند در معرض این آسیب‌پذیری قرار دارد.

راهکارهای امنیتی ارائه شده تا کنون

سیسکو تا کنون راهکاری برای این آسیب پذیری ارائه نداده است اما در به‌روزرسانی اخیر خود این آسیب‌پذیری را نیز تحت پوشش قرار داده است.

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۱۰۰۳-dna-auth-bypass

آسیب‌پذیری دسترسی بدون احراز هویت در مرکز معماری شبکه دیجیتال سیسکو

آسیب‌پذیری (گردآورنده: آتوسا خدامرادی)

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری Critical می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پذیری، با شناسه CVE-2018-15386، در مرکز معماری شبکه دیجیتال سیسکو (DNA) وجود داشته و به هکر احراز هویت نشده اجازه می‌دهد که فرآیند احرازهویت را دور زده و بدون اجازه، به توابع مدیریتی حیاتی دسترسی مستقیم پیدا کند.

آسیب‌پذیری یافت شده ناشی از پیکربندی

پیش‌فرض ناامن در سیستم آسیب‌دیده می‌باشد. هکر می‌تواند این آسیب‌پذیری را به وسیله ارتباط مستقیم با سرویس‌های در معرض خطر، اکسپلویت نماید. با اکسپلویت موفق این آسیب‌پذیری، هکر می‌تواند فایل‌های سیستمی حیاتی را بازیابی نموده و یا تغییر دهد.

محصولات آسیب‌پذیر

مرکز معماری شبکه دیجیتال سیسکو (DNA) نسخه ۱.۱ در معرض این آسیب‌پذیری قرار دارد.

راهکارهای امنیتی ارائه شده تا کنون

سیسکو تا کنون راهکاری برای این آسیب‌پذیری ارائه ننموده، اما در به‌روزرسانی اخیر خود این آسیب‌پذیری را نیز تحت پوشش قرار داده است.

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۱۰۰۳-dna-unauth-access

آسیب‌پذیری اجرای دستورات و بارگذاری فایل‌های دلخواه در Prime Infrastructure سیسکو

آسیب‌پذیری (گردآورنده: آتوسا خدامرادی)

شدت آسیب‌پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب‌پذیری Critical می‌باشد.

خلاصه آسیب‌پذیری

این آسیب‌پذیری با شناسه CVE-2018-15379، مربوط به وب سرور HTTP، برای Prime Infrastructure سیسکو (PI) می‌باشد و به موجب آن مجوز دسترسی نامحدودی برای دایرکتوری‌ها فراهم می‌شود که به یک هکر احراز هویت نشده اجازه می‌دهد از راه دور فایل‌های دلخواه خود را بارگذاری نماید.

این آسیب‌پذیری از تنظیمات غلط مجوز دسترسی، برای دایرکتوری‌های مهم سیستم ناشی می‌شود. هکر می‌تواند با بارگذاری یک فایل مخرب در TFTP این آسیب‌پذیری را اکسپلویت نماید، و به رابط گرافیکی وب دسترسی پیدا کند. اکسپلویت موفق این آسیب‌پذیری به هکر اجازه می‌دهد که بدون احراز هویت، دستوراتی را در برنامه کاربردی هدف اجرا کند.

محصولات آسیب‌پذیر

اگر سرور TFTP فعال باشد و با تنظیمات پیش فرض کار کند، نرم‌افزارهای PI سیسکو از نسخه ۳.۲ تا ۳.۴ پیش از انتشار اولین نسخه اصلی آسیب‌پذیر خواهند بود.

راهکارهای امنیتی ارائه شده تا کنون

مدیران باید دسترسی به TFTP را از طریق رابط وب برای PI سیسکو غیرفعال سازند:

Administration > setting > system setting > server > TFTP

همچنین مدیران می‌توانند پروتکل‌های امنی مانند SCP و یا SFTP را جایگزین TFTP نمایند.

سیسکو به‌روزرسانی جدیدی ارائه داده است که این آسیب‌پذیری را تحت پوشش قرار می‌دهد.

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۱۰۰۳-pi-tftp

کشف آسیب پذیری روز صفرم در ابزار AnyDesk، هنگام پیش‌بارگذاری dll در ویندوز

آسیب‌پذیری (گردآورنده: محمد جلیلی)

آزمایشگاه FortiGuard Fortinet، یک آسیب پذیری با شناسه CVE-2018-13102 کشف نموده است، این آسیب‌پذیری مربوط به ابزار AnyDesk در هنگام پیش بارگذاری DLL در ویندوز می‌باشد.

AnyDesk در ویندوز یک ابزار اختصاصی برای ارتباط از راه دور دسکتاپ است که متعلق به AnyDesk Software GmbH می‌باشد. این نرم افزار امکان دسترسی از راه دور به کامپیوترهای شخصی که برنامه میزبان را در حال اجرا دارند، فراهم می‌کند و در سیستم عامل‌های ویندوز، مکینتاش، لینوکس، FreeBSD، اندروید و IOS قابل اجرا می‌باشد.

ابزار AnyDesk در ویندوز، هنگام پیش‌بارگذاری فایل DLL آسیب‌پذیر است. این مشکل زمانی ایجاد می‌شود که برنامه برای اجرا، به دنبال بارگذاری یک فایل DLL است، در این هنگام مهاجم یک فایل DLL مخرب را جایگزین می‌کند. این ابزار معمولاً مسیر مشخصی را برای پیدا کردن فایل DLL جستجو می‌کند. می‌توان به سادگی با استفاده از نوشتن یک فایل جدید یا بازنویسی فایل موجود، از این آسیب‌پذیری استفاده کرده و یک فایل DLL خارجی را اجرا نمود.

راه‌حل

کاربران باید آخرین آپدیت AnyDesk، ارائه شده توسط سایت رسمی آن را نصب نمایند.

منابع خبر:

https://fortiguard.com/zeroday/FG-VD-18-064

http://cve.mitre.org/cgi-bin/cve-name.cgi?name=CVE-2018-13102

مقالات آموزشی

چگونه یک خرید آنلاین مطمئن داشته باشیم و بتوانیم صفحات نامعتبر را شناسایی کنیم؟

مقالات آموزشی (گردآورنده: محمد جلیلی)

هر وسیله‌ای را آنلاین تهیه نکنید

وسایلی را به صورت آنلاین تهیه کنید که یک بار از نزدیک دیده، یا از آن استفاده کرده باشید و از اینکه نیاز شما را برآورده خواهد کرد مطمئن شوید.

از سایت‌های معتبر خرید کنید

سایت‌های معتبر دارای نماد اعتماد الکترونیکی هستند. نماد الکترونیکی برچسبی است که منحصراً توسط مرکز توسعه تجارت الکترونیکی وزارت صنعت، معدن و تجارت به کسب و کارهای اینترنتی احراز صلاحیت شده و قانون‌مند اعطا می‌شود و آرم آن به شکل زیر است:

لازم است بعد از دیدن این علامت در سایت بر روی آن کلیک کرده و ابتدا به تاریخ اعتبار و اطلاعات مندرج در آن توجه کنید. اگر اولین باری است که قصد دارید از یک سایت ناشناس دارای نماد الکترونیکی خرید کنید، ابتدا اطلاعات مندرج در سایتی که می‌خواهید از آن خرید کنید یادداشت کرده (روی آرم نماد الکترونیکی در سایت کلیک کنید) و به آدرس سایت احراز هویت نماد الکترونیکی به نشانی enamad.ir رفته و در بخش استعلام، اطلاعات اعلامی در سایت را با اطلاعات ثبت شده در وب‌سایت احراز هویت مقایسه کرده و از نبودن هرگونه مغایرتی اطمینان حاصل کنید.

این کار به شما اطمینان می‌دهد اطلاعات بانکی و شخصی شما در سایت محفوظ مانده و در صورت وجود هرگونه نارضایتی می‌توانید از مراجع ذی‌صلاح خواسته خود را پیگیری کنید.

چک کردن حالت امن درگاه خرید به‌صورت"https"

همـواره از مرورگـر اینترنـتی بـه روز اسـتفاده کنیـد. زمـانی که علامـت "https" در بالای نـوار آدرس مرورگر به رنـگ قرمـز نمایـش داده شـد بـه معنی عـدم ایمـنی لازم اسـت و نبایـد در چنیـن وضعیـتی بـه پرداخـت اینترنـتی اقدام کرد.

استفاده از رایانه و موبایل شخصی برای خرید

در صـورت امـکان از کافی‌نـت و دسـتگاه‌هایی کـه متعلـق بـه شـما نیسـتند بـرای خریـد آنلایـن اسـتفاده نکنیـد. در صـورت ضـرورت از کیبـورد مجـازی سیسـتم مذکـور و در سـایت بانـک هـم از کیبـورد مجـازی بانـک مربوطه استفاده کنید.

آدرس درگاه انتقالی را با آدرس اصلی بانک چک کنید

زمـانی کـه فراینـد خریـد تکمیل شـد، سـایت شـما را به یـکی از درگاه‌هـای پرداخـت الکترونیـکی منتقـل می‌کنـد، آنـگاه آدرس را کامـلاً بـا آدرس اصـلی بانـک مربوطـه مطابقـت دهیـد و توجـه کنیـد کـه ابتـدای آدرس مـورد نظـر بایـد دارای رمزگـذاری "https" باشـد و رنـگ آن قرمـز نبـوده و نبایـد کوچکتریـن اختلافـی بـا آدرس اصلی بانک داشته باشد.

سـارقان جدیـد یـا همـان هکرهـا یـک سـایت کـه از نظر ظاهـری کامـلاً مشـابه سـایت‌های بانـک هسـت طراحی کـرده و ضمـن فریـب افـراد، اطلاعاتشـان را سـرقت می‌کننـد و بـه طبـع آن حسـاب فریـب خـوردگان خـالی می‌شـود.

تشـخیص سـایت‌های تقلـبی چنـدان دشـوار نیسـت. کافـی اسـت آدرس پرداخـت الکترونیـک بانـک خـود را بـه درسـتی بشناسـید. چراکـه هیچ هکـری نمی‌توانـد آن را سرقت نماید.

در انتهـا در هـر بـازه‌ای بـه تعویـض رموز خریـد اینترنتی خـود بپردازیـد و از یـک رمـز بـرای حسـاب‌های مختلف خود استفاده نکنید.

حملات فیشینگ به درگاه های بانکی

بـه دو تصویـر زیـر دقـت کنیـد کاملاً مشـابه می باشـد و کمتـر کـسی می توانـد حـدس بزنـد کـه یـکی از آنهـا توسـط سـارقان طراحـی شـده اسـت. تصویـر اول متعلـق بـه درگاه پرداخـت بانـک ملت می‌باشـد و تصویر دوم توسـط یـک هکـر و بـا هـدف سـرقت اطلاعـات بانکی طراحی شده است:

درگاه بانک ملت

درگاه جعلی بانک ملت

ایـن سـایت توسـط هکـری طراحـی شـده اسـت کـه به بهانـه فـروش محصولات خـود، اطلاعـات بانکی افـراد را سرقت می‌نمود.

ایـن دو سـایت تشـابه زیـادی دارنـد کـه کمتـر کـسی تصـور می کنـد یـکی از آنهـا هیـچ ارتباطـی بـه بانـک ملـت نـدارد و تنهـا اطلاعـات شـما را بـه دسـت هکرهـا

می‌دهد.
هکر ها هر چقدر هم بامهارت باشند بازهم تشخیص سایت‌های تقلبی چندان دشوار نیست کافی است آدرس پرداخت الکترونیک بانک خود را به درستی بشناسید. چرا که هیچ هکری نمی‌تواند آن را سرقت نماید.
آدرس صحیح درگاه‌های پرداخت بانک‌ها از قرار زیر است:
بانک پارسیان:

https://www.pecco۲٤.com/

بانک ملی:

https://epayment.bmi.ir/epayment/

بانک سامان:

https://acquirer.samanepay.com/

بانک ملت:

https://pgw.bpm.bankmellat.ir/

بانک پاسارگاد:

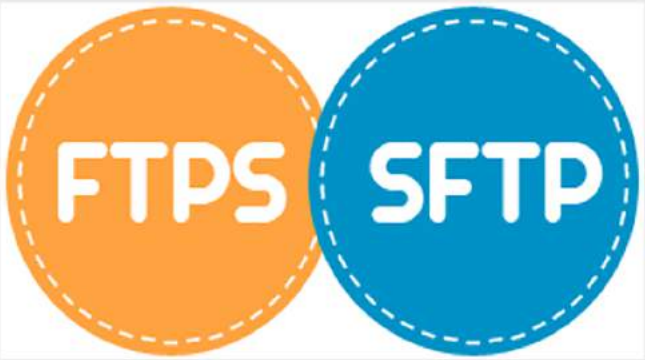
https://epayment.bankpasargad.com/

دومین راه تشخیص سایت‌های فیشینگ هم در قسمت URL سایت کاملاً واضح است. حتما دقت داشته باشید که در کنار آدرس سایت عبارت https:// ذکر شده باشد.
کارشناسان وجود علامت قفل مانند در کنار صفحات آدرس اینترنتی را هم در تشخیص اعتبار سایت مؤثر می‌دانند.

پس تنها در صورتی که به این دونکته ساده (آدرس پرداخت الکترونیک بانک و درج https در آدرس سایت) توجه کنید با خیالی راحت می توانید از خرید اینترنتی خود لذت ببرید.

مقایسه FTPS و SFTP

مقالات آموزشی (گردآورنده: سیده آرزو حسنی)



FTPS

در دهه ۹۰ میلادی نت اسکیپ پروتکل SSL را معرفی کرد که امروزه آن را به TLS هم میشناسیم، از SSL برای تبدیل FTP به FTPS استفاده می‌شود، FTPS هم مثل FTP از دو پورت یکی (۲۱) برای ارسال دستورات و دیگری (۲۰) برای تبادل دیتا استفاده می‌کند. در پروتکل FTPS برای احراز هویت از نام کاربری و پسورد یا Certificate یا از ترکیب هر دو استفاده می‌شود. زمان ارتباط با سرور FTPS ابتدا کلاینت Crtificate سرور را برای قابل اطمینان بودن چک می‌کند، این اطمینان در صورتی که Certificate توسط CA صادر شده باشد یا Self-Signed توسط سرور صادر شده باشد و کلاینت Public Certificate آن را داشته باشد حاصل می‌شود.

SFTP

در حالی که FTPS یک لایه را به پروتکل FTP اضافه

می‌کند، پروتکل SFTP یک تفاوت اساسی با FTPS دارد و آن هم این است که بر پایه پروتکل شبکه بنام SSH (Secure Shell) کار می‌کند و بر خلاف FTP و FTPS از یک تک کانال برای ارتباط، رمزگذاری و شناسایی و تبادل اطلاعات استفاده می‌نماید. SFTP از دو روش برای احراز هویت استفاده می‌کند، اولین روش مانند FTP از نام کاربری و پسورد استفاده می‌کند، بر خلاف FTP که این نام کاربری و پسورد را به صورت ساده ارسال و تائید می‌کند، در SFTP رمزگذاری می شود که برتری برجسته‌ای برای SFTP محسوب می‌شود.

روش احراز هویتی که در SFTP می‌توانید استفاده کنید SSH Key می‌باشد، این روش شامل ایجاد SSH private key و public key است، شما Public Key را ارسال نموده و روی SFTP سرور Load می‌شود و به اکانت شما تخصیص داده می‌شود، زمان ارتباط ابتدا توسط تطبیق Public Key و Private Key احراز هویت می‌شوید.

تفاوت FTPS وSFTP

ضمن اینکه هر دوی این پروتکل‌ها قوی هستند و مزایای خوبی دارند، اما تفاوت عمده آنها به شرح زیر است:

در FTPS از دو پورت استفاده می‌شود، ۲۱ برای ارسال دستورات و احراز هویت، و پورت ۲۰ نیز برای انتقال اطلاعات باید باز باشد، باز بودن این Port Range در فایروال برای شبکه شما ریسک امنیتی دارد، در حالی که SFTP از تک پورت شماره ۱۱ برای احراز هویت و انتقال اطلاعات استفاده می‌کند و این مسئله امن کردن آن را راحت‌تر می‌کند، همین مسئله باعث شده SFTP برای داشتن یک راهکار مدیریت انتقال فایل‌ها (Managed file transfer-MFT) مناسب‌تر است که توسط MFT می‌توانید، مانیتورینگ، و مدیریت داشته باشید.

امنیت کاربر رایانه

در زمان‌های گذشته معنای امنیت به امکان حفظ حیات و در امان ماندن از حیوانات، بلایا و یا حوادث طبیعی و مثال‌هایی ازین قبیل خلاصه می‌شده است، در جوامع کنونی مباحث گسترده‌ای در رابطه با موضوع امنیت مطرح هست که روز به روز به اهمیت این موضوع در بین افراد یا سازمان‌ها اضافه می‌شود.

با حضور ابزاری به نام کامپیوتر در چند دهه‌ی گذشته، دنیای امروز با انفجار حجم عظیمی از اطلاعات مواجه شده است، ازین رو امنیت این اطلاعات نیز غیر قابل انکار است، اطلاعات می‌تواند شامل هر چیزی باشد، تمام مواردی که یک شخص حقیقی و یا یک سازمان با آن در ارتباط است، امنیت یعنی با استفاده از یک سری فرآیندها از دسترسی غیرمجاز به اطلاعات و یا محصولات، و اعمال تغییرات یا حذف کردن آنها جلوگیری کنیم.

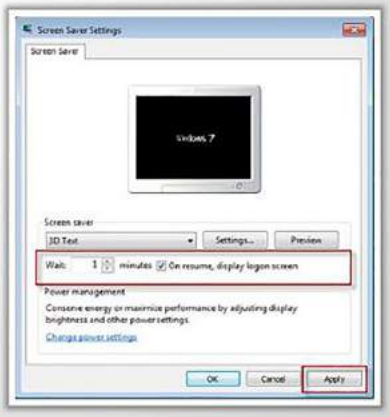
☑ در این شماره از بولتن خبری، در بخش "امنیت کاربر رایانه" قصد داریم در ادامه بحث شماره قبل، روش‌های حفظ امنیت در سیستم‌عامل‌ها را با هم مرور کنیم.

قفل نمودن سیستم زمانی که از آن استفاده نمی شود

به سه روش می توان سیستم را قفل نمود:

- فشردن همزمان کلیدهای Windows+L
- کلیک بر روی start در ویندوز -> Shut down -> Lock
- کلیک راست بر روی دسکتاپ، انتخاب گزینه Personalize، سپس انتخاب Screensaver

و پس از آن تیک زدن گزینه On resume display logon screen



ایجاد رمزعبور قوی

برای ایجاد پسورد به صورت زیر عمل نمایید:

Start-> Cntrol panel-> User Acconts-> Manage another account

بر روی نام کاربری که می خواهید پسورد آن را تغییر دهید کلیک نموده و **Create a password** را انتخاب نمایید (اگر پسورد قبلاً تنظیم شده باشد این گزینه **Change your password** خواهد بود)

در پنجره ایجاد پسورد، پسورد را تایپ نموده و آن را تأیید نمایید

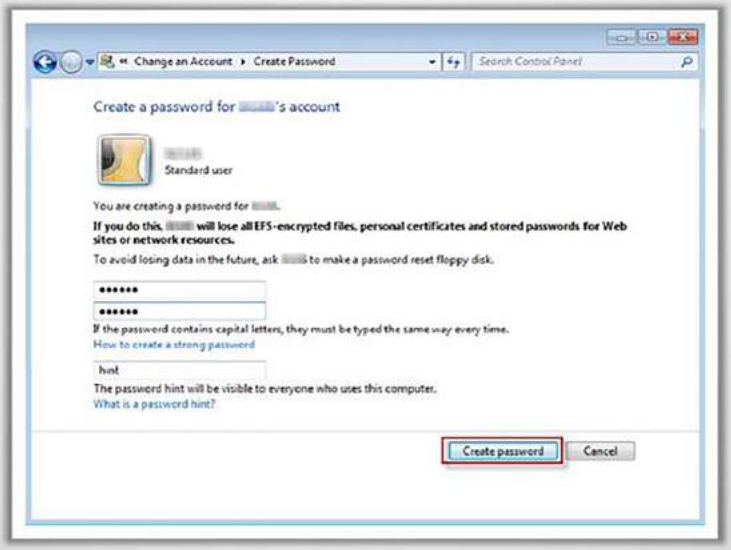
یک **password hint** مشخص کنید (اختیاری)

اگر پسورد قبلاً به حساب کاربری مورد نظر اختصاص داده شده باشد، و بخواهید آن را تغییر دهید ویندوز از شما می خواهد که پسورد فعلی را تأیید نمایید

بر روی دکمه **Create/Change Password** کلیک نمایید

نکته: برای ورود به سیستم از کلمات عبور قوی استفاده نمایید

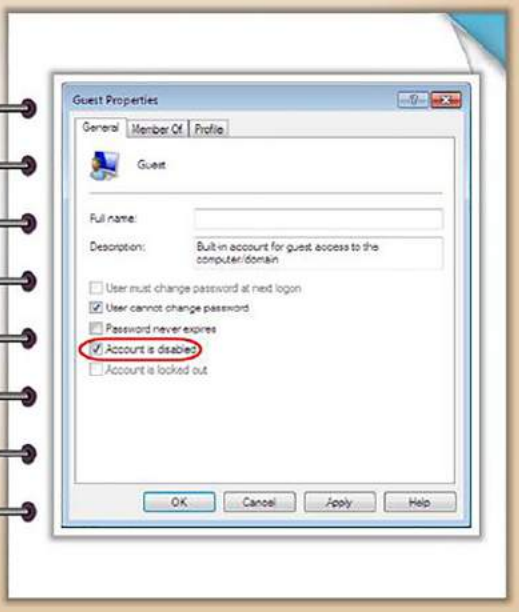
تغییر پسورد در ویندوز



غیرفعال نمودن حساب کاربری Guest

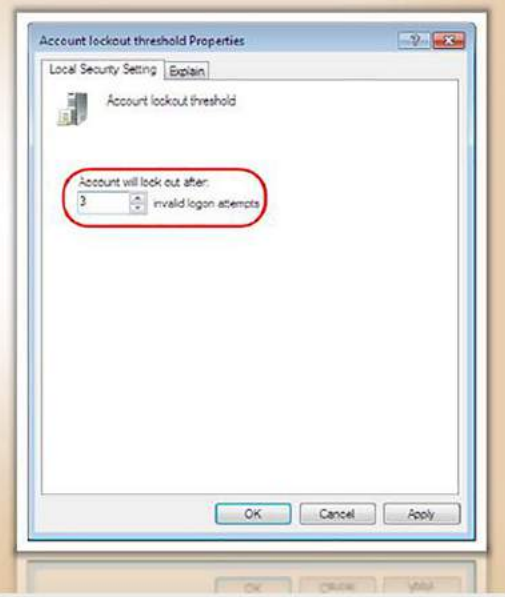
به منظور غیرفعال نمودن حساب کاربری Guest به صورت زیر عمل نمایید :

- بر روی Start کلیک نمایید، سپس بر روی Computer کلیک راست نموده وManage را انتخاب کنید
- زمانی که پنجره مدیریت کامپیوتر باز شد به قسمت Local Users and Groups، و سپسUser بروید
- به آیکون نگاه کنید و بررسی نمایید که آیا حساب کاربری Guest غیرفعال شده است یا خیر
- اگر حساب غیرفعال نشده بود بر روی نام حساب کاربری دابل کلیک نموده و پنجره تنظیمات آن را باز کنید
- در پنجره تنظیمات حساب کاربری Guest، تیک گزینه "Account is disabled"را بزنید



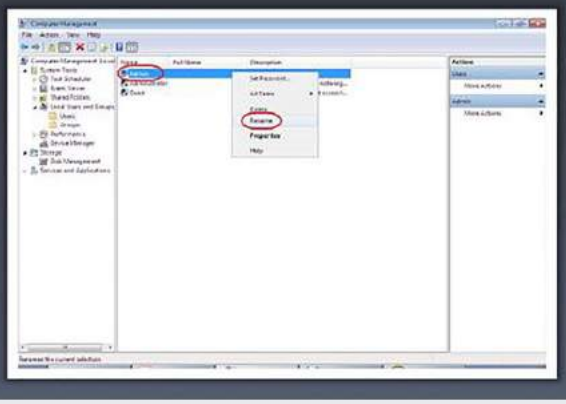
قفل نمودن حساب های Guest ناخواسته

- به Control panel رفته و بر روی Administrative Tools کلیک نمایید
- بر روی Local Security Policy دابل کلیک کنید، سپس Account را انتخاب نموده و بر روی Account Lockout Policy دابل کلیک نمایید، و پس از آن بر روی Account Lockout Threshold دابل کلیک کنید
- در تنظیمات Account lockout threshold تعداد ورودی های نامعتبر را وارد نمایید
- OK و سپس close را کلیک نمایید



تغییر نام حساب کاربری Administrator در ویندوز

از مسیر زیرپنجره Manage را در ویندوز باز کنید :
Start-> Computer-> Manage



در پنجره Computer Management بر روی Local Users and Groups کلیک نموده و سپس Users را انتخاب نمایید

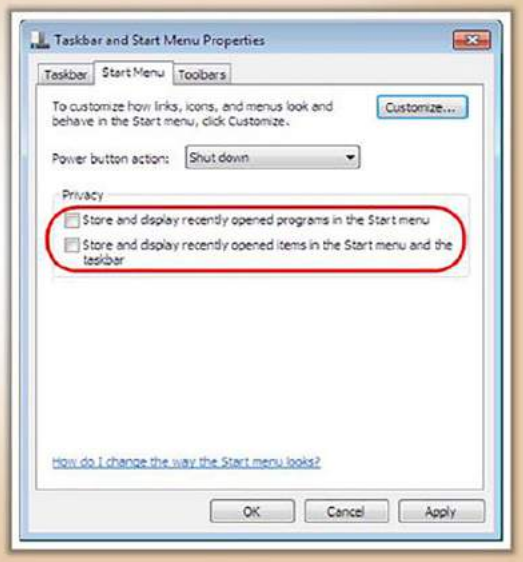
بر روی کاربر Admin یا Administrator کلیک راست نموده و Rename را انتخاب کنید، سپس نام جدیدی برای حساب کاربری وارد کرده و OK را بزنید

غیرفعال نمودن منوی Start up در ویندوز

بر روی Taskbar کلیک راست نموده و Properties را انتخاب کنید، در پنجره نشان داده شده به تب Start Menu بروید

تیک هر دو گزینه زیر را بردارید:

- Store and display recently opened programs in the Start menu
- Store and display recently opened items in the Start menu and the taskbar



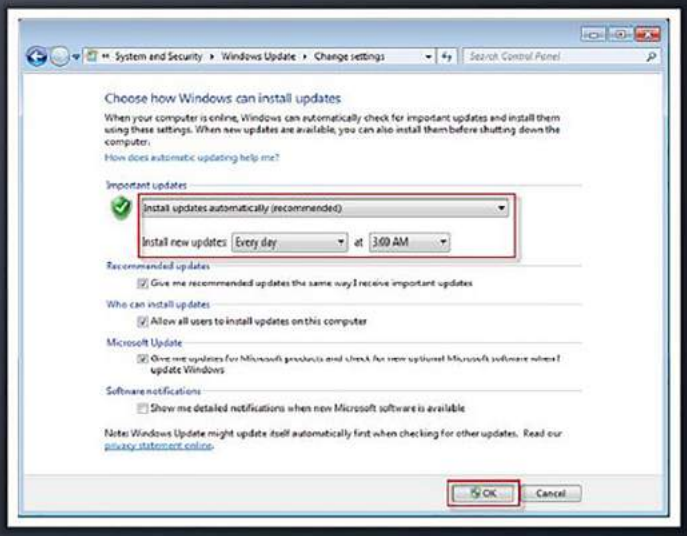
بروزرسانی در ویندوز

Windows Updates

در Control panel و System and Security را انتخاب کنید

Windows Update را انتخاب نموده و بر روی Change Setting کلیک نمایید

و در نهایت از قسمت Choose how Windows can install updates نحوه دریافت و نصب بروزرسانی ها را انتخاب نمایید



توصیه هایی در رابطه با بروزرسانی

ادامه این مبحث را در شماره‌های بعدی دنبال کنید...


مرکز تخصصی آپا دانشگاه اراک