بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و سوم

مرداد ماه ۱۳۹۹

افشا رمز عبور بیش از ۹۰۰ VPN سرور

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصی آپا دانشگاه رازی

صفحه آرایی: **علیرضا عبدی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری
سیده آرزو حسنی

آدرس:
کرمانشاه، باغ ابریشم، دانشگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

apa@razi.ac.ir
۰۸۳۳۴۳۴۳۲۵۱
@APARazi
cert.razi.ac.ir

اخبار امنیتی

نقص بحرانی در افزونه wpDiscuz وردپرس

در تاریخ 23 ژوئیه کارشناسان امنیتی Wordfence، یک آسیب‌پذیری با شدت بحرانی و CVSS base score 10 را در افزونه[1] wpDiscuz وردپرس کشف کردند و آن را به تیم توسعه wpDiscuz گزارش دادند، این افزونه بر روی بیش از 80,000 وب‌سایت مختلف نصب شده است.

نقص موجود در افزونه wpDiscuz وردپرس این امکان را به مهاجمان خواهد داد تا پس از بارگذاری فایل دلخواه بر روی سرور قربانی، کد دلخواه خود را از راه دور اجرا کرده و کنترل حساب کاربری قربانی را در دست گیرند. این افزونه به صورت آنی، امکان تفسیرِ Ajax را فراهم کرده و آن‌ها را در یک پایگاه‌داده محلی ذخیره می‌کند.

توسعه‌دهندگان در ابتدا با انتشار نسخه 7.0.4 موفق به رفع این نقص نشدند، اما در نهایت پس از انتشار نسخه 7.0.5، این آسیب‌پذیری به طور کامل برطرف شد.

محققان دریافتند که نسخه‌های وصله نشده افزونه wpDiscuz، در بررسی[2] انواع فایل های بارگذاری شده توسط کاربران ناموفق عمل کرده‌اند. این افزونه معمولا این امکان را به کاربران می‌دهد که تنها مجاز به پیوست[3] تصاویر باشند.

```
private function isAllowedFileType($mimeType) {
    $isAllowed = false;
    if (!empty($this->options->content["wmuMimeTypes"]) && is_array($this->
        $isAllowed = in_array($mimeType, $this->options->content["wmuMimeTy
    }
    return $isAllowed;
}
```

کد مربوط به فرآیند بارگذاری انواع فایل‌ها

افزونه wpDiscuz از جمله افزونه‌های محبوب و قدرتمند وردپرس جهت مدیریت نظرات کاربران[4] و سفارشی‌سازی آن‌ها می‌باشد؛ در واقع افزونه‌ای است که برای ایجاد فضای واکنش‌گرا یا responsive بخش نظرات در وب‌سایت های وردپرس طراحی شده است و به کاربران این امکان را خواهد داد تا درباره موضوعات بحث کنند و با استفاده از یک ویرایشگر قدرتمند متن، نظرات خود را ثبت نمایند، همچنین در افزونه‌های نسخه x.x.7، می‌توان تصویر دلخواه را در بخش نظرات ضمیمه کرد؛ اما متأسفانه پیاده‌سازی این ویژگی، ایمن نبوده و باعث بوجود آمدن آسیب‌پذیری بحرانی خواهد شد.

---

[1] plugin

[2] verify

[3] attach

[4] comments

مهاجم می‌تواند یک فایل مخرب را بر روی سرور میزبان سایت آسیب‌پذیر بارگذاری کرده و سپس با پاسخ به درخواست، مسیر فایل را برای اجرای آن روی سرور دریافت کرده و موفق به حمله اجرای کد از راه دور (RCE) گردد، این امر موجب می‌شود تا مهاجمان بتوانند هر نوع فایلی را ایجاد کرده و ویژگی‌های شناسایی تصویر را به فایل‌ها اضافه کنند تا از این طریق فرآیند اعتبار سنجی فایل را دور بزنند. یک فایل PHP که برای دور زدن فرآیند اعتبار سنجی مورد استفاده قرار می‌گیرد، می‌تواند چیزی شبیه به عبارت زیر را به عنوان یک درخواست درنظر گیرد:

```
------WebKitFormBoundaryXPeRFAXCS9qPc2sB

Content-Disposition: form-data; name="wmu_files[0]"; filename="myphpfile.php"

Content-Type: application/php

‰PNG
```

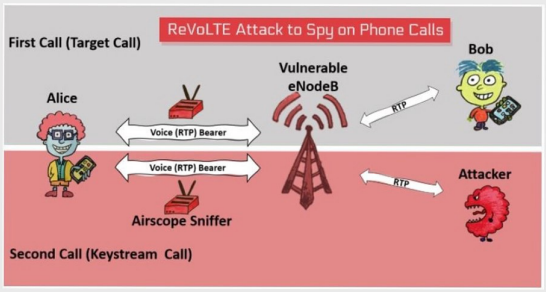
مسیر فایل به عنوان بخشی از پاسخ درخواست بازگردانده شده و کاربر این امکان را خواهد داشت که به راحتی مکان فایل را پیدا کرده و به فایلی که بر روی سرور بارگذاری شده است دسترسی پیدا کند؛ این بدان معنی است که مهاجمان می‌توانند فایل‌های PHP دلخواه را بارگذاری و سپس به آن‌ها دسترسی پیدا کنند تا بتوانند کد مورد نظر را از راه دور اجرا کرده و به هدف خود برسند.

با انتشار نسخه 7.0.5 افزونه wpDiscuz، تا 2 آگوست، حدود 40,000 مرتبه دانلود شده است و این بدان معناست که حداقل 40،000 سایت وردپرس تحت تأثیر این آسیب پذیری قرار گرفته‌اند.

منبع خبر :

Scan Link

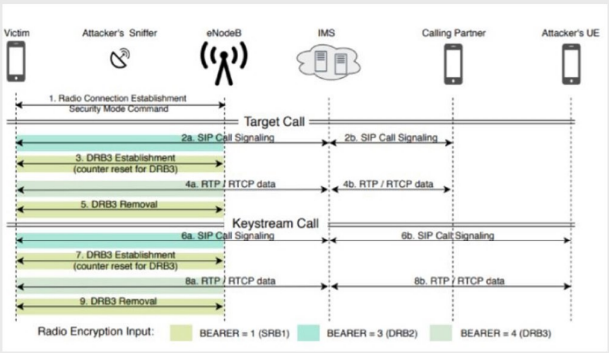
شنود مکالمات تلفن همراه و رمزگشایی پروتکل VoLTE



گروهی از محققان از حمله جدیدی به نام ReVoLTE پرده برداشتند که به مهاجمان این امکان را می‌دهد تا از راه دور رمزهای تماس صوتی VoLTE را شکسته و مکالمات قربانی را شنود کنند. این حمله هیچ نقصی را در پروتکل Voice over LTE (VoLTE) اکسپلویت نخواهد کرد ولی پیاده‌سازی ضعیف شبکه تلفن همراهLTE توسط اغلب ارائه‌دهندگان، به مهاجمان اجازه خواهد داد تا تماس‌های رمزشده قربانی را شنود کنند.

VoLTE یا پروتکل Voice over Long Term Evolution، در واقع یک ارتباط وایرلس استاندارد و با سرعت بالا برای تلفن‌های همراه و terminalها، از جمله دستگاه های مبتنی IOT [1] یا همان اینترنت اشیا و wearableها با استفاده از فناوری دسترسی رادیویی 4G LTE می‌باشد.

همانطور که در تصویر مشاهده می‌کنید، مشکلی که وجود دارد آن است که در یک ارتباط رادیویی، اکثر اپراتورها برای رمزگذاری داده‌های صوتیِ رد و بدل شده بین تلفن همراه و پایگاه آن [2] (مانند برج تلفن همراه) در دو تماس بعدی نیز، از keystream یکسان استفاده می‌کنند؛ بنابراین حمله ReVoLTE، همان keystream را از طریق پایگاه تلفن همراه آسیب‌پذیر، اکسپلویت می‌کند و به مهاجمان این امکان را خواهد داد تا محتویات تماس صوتی VoLTE را رمزگشایی کنند؛ به هرحال استفاده مجدد از یک keystream قابل پیش‌بینی که اولین بار توسط Raza & Lu به آن اشاره شد، مسئله جدیدی نیست اما حمله ReVoLTE، موجب خواهد شد تا این مسئله به یک حمله واقعی تبدیل شود.



نمودار ترتیبی ReVoLTE: رمزگذاری Target call به عنوان keystream یکسان با call keystream

برای شروع حمله ReVoLTE و در اولین مرحله، مهاجم باید به همان base station قربانی متصل شده و یک downlink sniffer [3] را جهت بررسی و ضبطِ targeted call جاساز کند و هنگامی که قربانی targeted call را قطع کرد، مهاجم باید بلافاصله در مدت زمان 10 ثانیه با قربانی تماس بگیرد که این امر باعث می‌شود شبکه آسیب‌پذیر مجدداً یک تماس جدید بین قربانی و مهاجم را در همان ارتباط رادیویی برقرار کند. در مرحله دوم حمله، پس از برقراری ارتباط، مهاجم باید قربانی را درگیر مکالمه کرده و مکالمات را در قالب متن ضبط کند، این روند به مهاجم کمک خواهد کرد تا key-stream بکاررفته در تماس بعدی را محاسبه‌ی معکوس کند.

گفتنی است برای رمزگشایی هر فریم، باید طول تماس دوم، بیشتر یا مساوی اولین تماس باشد، زیرا در غیر این صورت مهاجم تنها بخشی از مکالمه را می‌تواند رمزگشایی کند؛ یعنی مهاجم مجبور است قربانی را درگیر گفتگوی طولانی‌تری کند و هرچه بیشتر با قربانی صحبت کند، محتوای ارتباط قبلی او بیشتر رمزگشایی خواهد شد.

به گفته محققان، استفاده مجدد از keystream هنگامی رخ می‌دهد که هدف و call keystream از همان کلید رمزگذاری استفاده می‌کنند. از آنجایی که این کلید برای هر ارتباط رادیویی جدید بروزرسانی می‌شود، مهاجم باید مطمئن شود که اولین بسته از key-stream call، پس از target call وارد فاز فعال [4] خواهد شد.

---

[1] Internet of things

[2] base station

[3] اسنیفر برنامه یا ابزاری است برای شنود ترافیک شبکه آن هم بوسیله گرفتن اطلاعاتی که روی شبکه در حال تبادل هستند، استفاده می‌شود.

[4] active phase

از آنجا که این نقص بسیاری از شرکت‌های ارائه دهنده خدمات ارتباطی را تحت تأثیر قرار می‌دهد، محققان امنیتی یک اپلیکیشن اندورید open source منتشر کردند که از طریق آن می‌توان تشخیص داد شبکه و یا پایگاه‌های G4 آن‌ها در برابر حمله ReVoLTE آسیب پذیر است یا خیر.

منبع خبر :

Scan Link

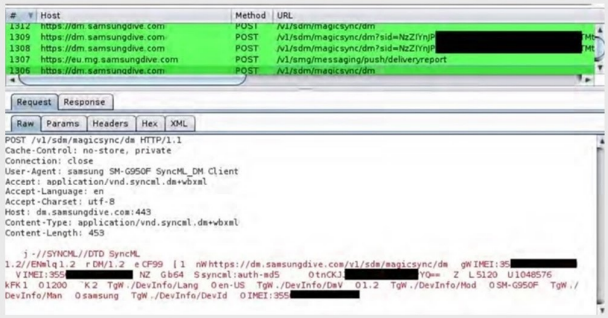
افشای آسیب‌پذیری در گوشی‌های سامسونگ

تحقیقات جدید وجود مجموعه‌ای از آسیب‌پذیری‌های امنیتی با شدت بالا در 'Find My Mobile' را نشان می‌دهد که مهاجمان از راه دور را قادر می‌سازد تا مکان واقعی قربانیان را ردیابی کنند، مکالمات تلفنی و پیامک‌ها را پایش کنند و حتی داده‌های ذخیره شده در تلفن را حذف نمایند. Find My Mobile یک برنامه مخصوص سیستم‌عامل اندروید است که در اکثر تلفن‌های هوشمند سامسونگ، از پیش نصب شده است.

این نقص امنیتی به راحتی می‌تواند مورد بهره‌برداری قرار گیرد و پیامدهای شدیدی برای کاربران به دنبال داشته باشد از جمله: انکار سرویس[1] دائمی از طریق قفل تلفن همراه، از بین رفتن کامل داده‌ها با برگشت به تنظیمات کارخانه[2] (شامل کارت SD)، پیامدهای جدی حریم خصوصی از طریق IMEI و ردیابی موقعیت مکانی و همچنین دسترسی به تماس‌ها و پیامک‌ها.

آسیب‌پذیری‌های مذکور، گوشی‌های سامسونگ مدل گلکسی S7، S8 و S9+ را تحت تأثیر قرار می‌دهند. سرویس Find My Mobile به صاحبان دستگاه‌های سامسونگ این امکان را می‌دهد تا از راه دور تلفن همراه یا تبلت خود را ردیابی یا قفل کنند، از داده‌های ذخیره شده بر روی دستگاه در Samsung Cloud نسخه پشتیبان تهیه کنند، داده‌های local را پاک کنند و دسترسی به Samsung Pay را مسدود کنند.

چهار آسیب‌پذیری مختلف در این اپلیکیشن وجود دارد که می‌تواند توسط یک برنامه مخرب نصب شده بر روی دستگاه هدف مورد سوء استفاده قرار بگیرد، بنابراین یک حمله man-in-the-disk برای ربودن ارتباطات از سرورهای پشتیبان و مخفیانه بر روی دستگاه قربانی ایجاد می‌شود.



این نقص امنیتی ناشی از این است که این برنامه یک فایل خاص را بر روی کارت SD دستگاه ("/mnt/sdcard/fmm.prop")، به منظور بارگزاری یک URL[3]، بررسی می‌کند بنابراین به یک برنامه جعلی اجازه می‌دهد تا این فایل را که می‌تواند توسط یک مهاجم برای ربودن ارتباطات با سرور مورد استفاده قرار گیرد، ایجاد کند.

با نشان دادن MG URL به یک سرور کنترل‌شده توسط مهاجم و اجبار کردن فرآیند ثبت نام[4]، مهاجم می‌تواند اطلاعات بسیاری را در مورد کاربر بدست آورد، از جمله: موقعیت مکانی از طریق آدرس آی‌پی، IMEI، نام تجاری دستگاه، سطح API، اپلیکیشن‌های پشتیبان‌گیری و اطلاعات دیگر.

برای دستیابی به این هدف، یک برنامه مخرب نصب شده بر روی دستگاه از یک زنجیره اکسپلویت استفاده می‌کند که از دو گیرنده محافظت نشده برای هدایت دستورات ارسال شده به سرورهای سامسونگ از برنامه Find My Mobile به سرور دیگری که تحت کنترل مهاجم است و دستورات مخرب را اجرا می‌کند، استفاده می‌کند.

این سرور مخرب همچنین این درخواست را به سرور اصلی ارسال می‌کند و پاسخ را بازیابی می‌کند اما نه قبل از تزریق دستورات خود در پاسخ‌های سرور. با انجام این کار، یک حمله موفقیت آمیز می‌تواند به یک هکر اجازه دهد تا موقعیت مکانی دستگاه را ردیابی کند، اطلاعات تماس و پیام‌های متنی را برای جاسوسی ضبط کند، تلفن را به منظور دریافت باج قفل کند و تمام داده‌ها را از طریق بازگشت تنظیمات به حالت کارخانه پاک کند.

منبع خبر :

Scan Link

اخبار کوتاه

شهروندان مراقب کلاهبرداری در پوشش نذری اینترنتی باشند

شهروندان مراقب باشند فریب مجرمان سایبری را نخورند و برای کمک به افراد بی‌بضاعت یا بیماران نیازمند حتما از طریق سایت‌های مؤسسات معتبر اقدام کنند و به هیچ عنوان به پیام‌ها یا کانال‌های راه افتاده در شبکه‌های اجتماعی اطمینان نکنند. در پی تبلیغات جمع‌آوری نذورات و کمک برای نیازمندان شاهد ارسال لینک‌های جعلی در کانال‌ها و شبکه‌های‌اجتماعی هستیم که با سرقت اطلاعات بانکی شهروندان حساب بانکی آن‌ها را خالی می‌کنند. حتماً برای هرگونه واریز وجه جهت نذر و کمک خود به قشر آسیب دیده، فقط از طریق شماره حساب‌های نهادهای معتبر و سازمان‌های مربوطه اقدام نمایند و از پرداخت‌های اینترنتی از طریق شبکه‌های اجتماعی به افراد ناشناس جدا خودداری کنند.

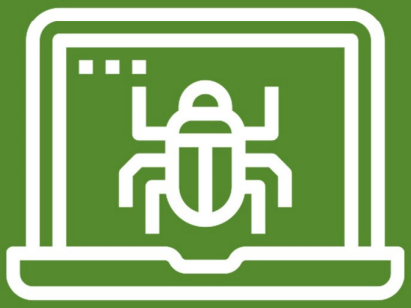
---

[1] denial of service

[2] factory reset

[3] ("mg.URL")

[4] registration



آسیب‌پذیری

رفع 5 آسیب‌پذیری بحرانی در روترهای D-Link

شرکت D-Link به رفع پنج آسیب‌پذیری موثر بر روی روترهای این شرکت با شدت‌های متوسط، بالا و بحرانی پرداخته است. با اکسپلویت این آسیب‌پذیری‌ها توسط مهاجمان، روترهای آسیب‌پذیر و به دنبال آن، شبکه به خطر خواهد افتاد. متأسفانه برخی از روترهای تحت تأثیر این آسیب‌پذیری‌ها، به وضعیت‌های EOS [1] و یا EOL [2] رسیده و این شرکت دیگر از آن‌ها پشتیبانی نخواهد کرد و این بدان معناست که بروزرسانی‌های امنیتی را نیز دریافت نخواهند کرد.

برا اساس گزارش‌های منتشر شده، روترهای DAP-1522 و DIR-816L که از جانب شرکت D-Link پشتیبانی نمی‌شوند، تحت تأثیر این آسیب‌پذیری‌ها قرار دارند. این دستگاه‌ها، فریمورهای نسخه v1.42 و v12.06.B09 و قبل‌تر را اجرا می‌کنند و در حال حاضر بروزرسانی‌های امنیتی منتشر شده را دریافت نخواهند کرد.

آسیب‌پذیری‌های مورد بحث، توسط تیم ACE، از شرکت Loginsoft گزارش داده شده اند که در ادامه در خصوص جزئیات فنی هر یک از آن‌ها بیشتر توضیح داده خواهد شد، گفتنی است که برخی از این نقص‌ها در 9 فوریه 2019 و برخی دیگر نیز در مارس 2020 گزارش داده شدند؛ اما همه آن‌ها در 22 جولای 2020 به طور عمومی منتشر شدند.

1. CVE-2020-15892

این نقص یک آسیب‌پذیری سرریز بافر مبتنی بر پشته کلاسیک در D-LINK Firmware DAP 1520 می‌باشد که شدت بحرانی و Base Score 9.8 به آن اختصاص داده شده است.

Extender یک گسترش‌دهنده محدوده وایرلس قابل حمل [3] است که به کاربران امکان می‌دهد منطقه پوشش شبکه وایرلس موجود را توسعه و گسترش دهند. کاربران می‌توانند برای افزایش دامنه شبکه وایرلس خود آن را در هر نقطه از خانه یا محل کار قرار دهند.

نسخه‌های آسیب‌پذیر Firmware، 1.0.8 و 1.10B0 هستند. این آسیب‌پذیری در D-link DAP 1520 access point، در 'ssi' binary وجود دارد و منجر به اجرای دستورات دلخواه می‌شود.

زمانیکه که کاربر از طریق رابط وب اقدام به ورود به سیستم می‌کند، مقادیر درخواست به 'ssi' binary ارسال می‌شوند. در صفحه ورود، رابط وب طول ورودی رمزعبور را به 15 کاراکتر محدود می‌کند. مشکل ناشی از آن است که

[1] End-of-Support
[2] End-of-Life
[3] portable Wireless Range Extender

اعتبارسنجی کاربر از طرف کلاینت انجام می‌شود، از این جهت زمانیکه یک مهاجم موفق به رهگیری درخواست ورود به سیستم (POST based) می‌شود و از پارامتر آسیب‌پذیر (`log_pass`) برای افزایش طول رمزعبور استفاده کند، این اعتبارسنجی می‌تواند دور زده شود و درخواست به وب سرور ارسال گردد. تعداد کمی از متغیرهای POST که به عنوان بخشی از درخواست ورود به سیستم منتقل می‌شوند، آسیب‌پذیر هستند که عبارتند از: `ht-ml_response_page` و `log_user`.

روش بهره‌برداری

مهاجم می‌تواند هر کسی باشد که به شبکه متصل شده است و قادر است به صفحه ورود روتر دسترسی داشته باشد. در این صورت می‌تواند پی‌لود [1] مورد نظر را در فیلدهای آسیب‌پذیر رابط وب وارد کرده و اقدام به اجرای دستورات دلخواه نماید.

روش‌های کاهش/رفع

- بررسی طول رمزعبور باید در سمت سرور انجام گیرد.
- در صورت عدم اعتماد به ورودی، حافظه باید به صورت پویا تخصیص یابد.

2. CVE-2020-15893

این نقص یک آسیب‌پذیری تزریق دستور در روترهای DIR-816L با شدت بحرانی و Base Score 9.8 است که به مهاجم اجازه می‌دهد از طریق یک پکت جعلی M-SEARCH، دستورات دلخواه خود را به UPnP تزریق کند. Universal Plug and Play (UPnP) به طور پیش‌فرض در DIR-816L و در پورت 1900 فعال شده است. مهاجم می‌تواند این حمله را با تزریق پی‌لود در قسمت 'Search Target' (ST) مربوط به SSDP M-SEARCH discover packet انجام دهد.

روش بهره‌برداری

مهاجم می‌تواند هر شخصی باشد که به شبکه متصل شده است و قادر به ارسال درخواست به پورت UPnP است. یک پکت جعلی و دستکاری‌شده می‌تواند از طریق نوشتن یک اسکریپت پایتون ساده، که به نوبه خود دستورات تهیه شده را به عنوان بخشی از درخواست جعلی اجرا می‌کند، به پورت ویژه upnp ارسال شود. POC به اشتراک گذاشته شده، سرویس telnet را بر روی پورت 8089 روشن کرده و یک gateway را برای ورود مهاجم فراهم می‌کند.

روش‌های کاهش/رفع

- برای فیلترکردن پی‌لودهای مرتبط به تزریق دستور، از روش لیست سیاه یا Blacklist استفاده شود، مانند `';`، `||` و غیره.

3. CVE-2020-15894

این نقص در روترهای DIR-816L با شدت بالا و با Base Score 7.5 اعلام شده است. در بهره‌برداری از این آسیب‌پذیری مهاجم می‌تواند هر شخصی باشد که به شبکه متصل است و همچنین قادر است به صفحه ورود روتر دسترسی داشته باشد.

روش بهره‌برداری

نقص مذکور در تابع administration افشا شده در getcfg.php که می‌تواند برای تماس با سرویس‌های مختلف مورد استفاده قرارگیرد، وجود دارد و به واسطه آن، مهاجم می‌تواند دسترسی غیرمجاز به برخی اطلاعات حساس را بدست آورد.

مهاجم برای این حمله باید به اطلاعات ورود مدیر (رمز عبور هش شده) دست یابد.

روش‌های کاهش/رفع

- قبل از هر دسترسی به عملکردهای سطح مدیریتی باید سشن به صورت درست بررسی شود.

4. CVE-2020-15895

این نقص یک آسیب‌پذیری Reflected Cross-site scripting با شدت متوسط و Base Score 6.1 در روتر DIR-816L است که ناشی از چاپ مقدار "RESULT" در صفحه وب می‌باشد.

روش بهره‌برداری

برای اکسپلویت این آسیب‌پذیری، مهاجم می‌تواند به صورت محلی و یا از راه دور به شبکه متصل شود و با فریب قربانی به بازید از یک لینک جعلی، کوکی [2] فعلی قربانی را به سرور مهاجم ارسال کند. اما به منظور اکسپلویت کامل این آسیب‌پذیری، مهاجم باید در یک شبکه محلی قرار گیرد تا کوکی سرقت شده را به مرورگر تزریق کند و session قربانی را به سرقت برد.

روش‌های کاهش/رفع

- برای حذف کاراکترهای اضافی باید جداسازی (escaping) مناسب خروجی انجام گیرد.

5. CVE-2020-15896

این آسیب‌پذیری با شدت بالا و Base Score 7.5 مربوط به دور زدن احراز هویت در روتر D'link DAP 1522 access point است و به مهاجم اجازه می‌دهد تا به رابط وب [3]، دسترسی غیرمجاز پیدا کند.

روش بهره‌برداری

مهاجم می‌تواند هر شخصی باشد که به شبکه متصل است و قادر است به صفحه ورود روتر دسترسی داشته باشد تا از این طریق آسیب‌پذیری را اکسپلویت کند. گفتنی است که به واسطه این آسیب‌پذیری، مهاجم می‌تواند به اطلاعات حساس دسترسی پیدا کند.

شرکت D-Link، فریمور Exceptional Beta Patch Release نسخه v1.10b04Beta02 را برای مدل D-Link DAP-1520 که فریمور آسیب‌پذیر نسخه v1.10B04 را اجرا می‌کنند، منتشر کرد. لذا با توجه به اهمیت آسیب‌پذیری‌های مذکور و بالا بودن شدت آن‌ها، هرچه سریع‌تر نسبت به وصله این آسیب‌پذیری‌ها، اقدام کنید.

منبع خبر :

Scan Link

[1] payload
[2] cookie
[3] web interface

آسیب‌پذیری اجرای کد از راه دور در Microsoft Sharepoint Server

طبق گزارشات منتشر شده، یک آسیب‌پذیری اجرای کد از راه دور در Microsoft Sharepoint Server وجود دارد که هنگام عدم موفقیت در شناسایی درست و فیلتر کردن صفحات وب ASP.Net ناامن رخ می‌دهد. یک مهاجم احراز هویت شده که بتواند با موفقیت از آسیب‌پذیری سوءاستفاده کند، با استفاده از یک صفحه جعلی می‌تواند در بستر امن SharePoint application pool اقدامات مخرب انجام دهد.

هفته‌ی گذشته، مایکروسافت برای اصلاح آسیب‌پذیری با شناسه CVE-2020-1181 و شدت خطر CVSS 8.8 یک وصله‌ی امنیتی منتشر نمود. این آسیب‌پذیری در واقع یک اشکال اجرای کد از راه دور در نسخه‌های پشتیبانی شده‌ی Microsoft SharePoint Server است که برای مهاجم احراز هویت شده امکان اجرای کد دلخواه .NET را فراهم می‌آورد. به منظور اجرای موفقیت‌آمیز حمله، مهاجم باید مجوزهای صفحاب وب را در سایت SharePoint اضافه کرده و یا سفارشی نماید.

از طرفی نیز پیکربندی پیش‌فرض SharePoint به کاربران مجاز، امکان ایجاد سایت را خواهد داد. این بدان معناست که کاربر پس از ایجاد سایت، مالک آن بوده و تمام مجوزهای لازم را در اختیار خواهد داشت.

آسیب‌پذیری مذکور بر روی PAN-OS 9.1 و نسخه‌های قبل از PAN-OS 9.1.3، PAN-OS 9.0 و نسخه‌های قبل از PAN-OS 9.0.9 و PAN-OS 8.1، نسخه های قبل از PAN-OS 8.1.15 و تمام نسخه‌های PAN-OS 8.0 (EOL) تأثیر می گذارد، گفتنی است که این آسیب‌پذیری بر روی PAN-OS 7.1 تأثیر نمی‌گذارد.

برای اکسپلویت این آسیب‌پذیری، کاربری که احراز هویت شده است باید یک صفحه ساختگی خاص را بر روی یک نسخه از Microsoft SharePoint Server ایجاد کند تا مهاجم از این طریق بتواند حملات مخرب خود را از سرگرفته، سیستم را مختل کند و نهایت به هدف خود برسد.

لیست محصولات تحت تأثیر این آسیب‌پذیری در جدول زیر آورده شده است:

محصولات تحت تأثیر	روش اعمال آسیب‌پذیری	شدت آسیب‌پذیری
Microsoft SharePoint Enterprise Server 2016	اجرای کد از راه دور	بحرانی
Microsoft SharePoint Server 2019	اجرای کد از راه دور	بحرانی
Microsoft SharePoint Foundation 2010 Service Pack 2	اجرای کد از راه دور	بحرانی
Microsoft SharePoint Foundation 2013 Service Pack 1	اجرای کد از راه دور	بحرانی

لیست محصولات تحت تأثیر این آسیب‌پذیری

گفتنی است کاربران می‌توانند جهت دانلود بروزرسانی‌های مربوط به هر یک از محصولات تحت تأثیر این آسیب‌پذیری، به مسیر /en-us/download/ در سایت مایکروسافت مراجعه کرده و نسبت به دانلود هر یک از آن‌ها اقدام نمایند.

راهکار

در حالت کلی مشتریان می‌توانند موارد زیر را بررسی کنند تا مشخص شود که آیا تحت تاثیر آسیب‌پذیری مذکور قرار گرفته‌اند یا خیر:

- لاگ‌های احراز هویت
- لاگ‌های User-ID
- ACC Network Activity Source/Destination Regions (Leveraging the Global Filter feature)
- Custom Reports (Monitor > Report)
- لاگ‌های GlobalProtect (در نسخه PAN-OS 9.1.0 و بالاتر)

اما با توجه به اهمیت این آسیب‌پذیری و نیز بالا بودن شدت آن، هرچه سریع‌تر نسبت به وصله دستگاه‌های تحت تأثیر این آسیب‌پذیری بخصوص اگر پروتکل SAML مورد استفاده قرار گرفته است، اقدام کنید. این بروزرسانی امنیتی، با اصلاح چگونگی مدیریت Microsoft SharePoint Server ، منجر به رفع این آسیب‌پذیری می‌شود.

منبع خبر :

Scan Link

رفع چندین آسیب‌پذیری بحرانی در محصولات سیسکو

شرکت سیسکو در تاریخ 29 جولای سال 2020، با انتشار چند بروزرسانی امنیتی، چندین آسیب‌پذیری را وصله زد؛ این آسیب‌پذیری‌ها با شناسه‌های CVE-2020-3375، CVE-2020-3382 و CVE-2020-3374 به ترتیب مربوط به دور زدن فرآیند احراز هویت [1]، سرریز بافر و دورزدن فرآیند تخصیص منابع [2] می‌باشند؛ علاوه بر این شرکت سیسکو در تاریخ 17 جون سال 2020 برای برخی آسیب پذیری‌های بحرانی مربوط به Treck IPstack، با شناسه‌های CVE-2020-11896 تا CVE-2020-11914، بروزرسانی v1.7 را منتشر کرد.

این شرکت به روزرسانی‌های امنیتی دیگری را برای رفع 8 آسیب‌پذیری با شدت بالا و متوسط که بر روی چندین نسخه نرم افزار [3] DCNM تأثیر می‌گذارند، منتشر کرد، شناسه این آسیب‌پذیری‌ها عبارتند از:

[1] authentication
[2] authorization
[3] Cisco Data Center Network Manager

CVE-2020-3377, CVE-2020-3384, CVE-2020-3383,
CVE-2020-3386, CVE-2020-3376, CVE-2020-3460,
CVE-2020-3462, CVE-2020-3461

• CVE-2020-3375

این آسیب‌پذیری با شدت بحرانی و Base Score 9.8 نرم‌افزار Cisco SD-WAN Solution Software را تحت تأثیر قرار می‌دهد و به مهاجم اجازه می‌دهد تا منجر به سرریز بافر از راه دور بر روی دستگاه‌های تحت تأثیر شود، در واقع این آسیب‌پذیری ناشی از اعتبارسنجی[1] نادرست ورودی می‌باشد. مهاجم غیر مجاز با ارسال ترافیک ساختگی به یک دستگاه تحت تأثیر این آسیب‌پذیری، می‌تواند آن را اکسپلویت کرده و پس از اکسپلویت موفقیت‌آمیز این آسیب‌پذیری، می‌تواند به اطلاعاتی که مجوز دسترسی به آن‌ها را ندارد دسترسی پیدا کرده، تغییراتی را در سیستم اعمال کند که در واقع مجاز به انجام آن ها نیست و دستوراتی را با سطح دسترسی root در سیستم تحت تأثیر این آسیب‌پذیری اجرا کند.

این آسیب‌پذیری در صورت اجرای یک نسخه آسیب‌پذیر از نرم‌افزار Cisco SD-WAN Solution بر روی محصولات زیر تأثیر خواهد گذاشت:

- IOS XE SD-WAN Software
- SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Cloud Routers
- SD-WAN vEdge Routers
- SD-WAN vManage Software
- SD-WAN vSmart Controller Software

مشتریانِ محصولات سیسکو هر چه سریع‌تر، نرم‌افزارهای موجود در جدول‌های ارائه شده را به نسخه وصله شده ارتقاء دهند.

نسخه‌های وصله شده نرم‌افزارCisco SD-WAN vManage Software برای آسیب‌پذیری با شناسهCVE-2020-3375

First Fixed Release	Cisco SD-WAN vManage Software Release
ارتقاء به نسخه وصله شده قبلی	18.3.0
18.4.5	18.4.0
19.2.3	19.2.0
ارتقاء به نسخه وصله شده قبلی	19.3.0
20.1.1	20.1.0

نسخه وصله شده نرم‌افزارهای Cisco SD-WAN vEdge, vBond و vSmart برای آسیب‌پذیری با شناسه CVE-2020-3375

First Fixed Release	Cisco SD-WAN vEdge, vBond and vSmart Software Releases
ارتقاء به نسخه وصله شده قبلی	18.3.0
18.4.5	18.4.0
19.2.3	19.2.0
ارتقاء به نسخه وصله شده قبلی	19.3.0
20.1.1	20.1.0

• CVE-2020-3374

این آسیب‌پذیری با شدت بحرانی و Base Score 9.9 در رابط مدیریت مبتنی بر وب نرم افزار Cisco SD-WAN vManage وجود دارد و به مهاجم اجازه می‌دهد تا از راه دور، فرآیند تخصیص منابع[2] را دور زده و به اطلاعات حساس دسترسی پیدا کند، پیکربندی سیستم را تغییر دهد و به سیستم تحت تأثیر، لطمه بزند. این آسیب‌پذیری در واقع ناشی از بررسی نادرست دسترسی و تخصیص منابع در سیستم تحت تأثیر این آسیب پذیری می‌باشد. مهاجم می‌تواند با ارسال یک درخواست HTTP ساختگی به رابط مدیریت مبتنی بر وبِ دستگاه تحت تأثیر، این آسیب‌پذیری را اکسپلویت کند؛ پس از اکسپلویت موفقیت‌آمیز این آسیب‌پذیری، مهاجم فراتر از حد معمول، اجازه پیکربندیِ تخصیص منابع کاربران را خواهد داشت.

گفتنی است این آسیب‌پذیری در صورت اجرای یک نسخه آسیب‌پذیر از نرم‌افزار Cisco SD-WAN vManage بر روی دستگاه‌های سیسکو تأثیر خواهد گذاشت و به مشتریانِ محصولات سیسکو توصیه می‌شود هر چه سریع‌تر، نرم‌افزارهای موجود در جدول 4 را به نسخه وصله شده ارتقاء دهند.

نسخه‌های وصله شده نرم‌افزارCisco SD-WAN vManage Software برای آسیب‌پذیری با شناسه CVE-2020-3374

First Fixed Release	Cisco SD-WAN vManage Software Release
ارتقاء به نسخه وصله شده قبلی	Earlier than 18.3
ارتقاء به نسخه وصله شده قبلی	18.3
18.4.5	18.4
19.2.2	19.2
ارتقاء به نسخه وصله شده قبلی	19.3
20.1.1	20.1

• CVE-2020-3382

این آسیب‌پذیری با شدت بحرانی و Base Score 9.8 در REST API مربوط به نرم افزار (Data Center Network Manager (DCNM شرکت سیسکو، به یک مهاجم غیر مجاز اجازه می‌دهد تا از راه دور فرآیند احراز هویت را دور زده و کدهای دلخواه خود را با سطح دسترسی administrative بر روی دستگاه آسیب‌پذیر اجرا کند. این آسیب‌پذیری ناشی از نصب‌های مختلفی است که دارای یک کلید رمزگذاری استاتیک هستند. مهاجم می‌تواند آسیب‌پذیری مذکور را با استفاده از کلید استاتیک برای ایجاد یک توکن session معتبر، اکسپلویت نماید. مهاجم پس از یک اکسپلویت موفق می‌تواند اقدامات دلخواه خود را از طریق REST API با سطح دسترسی administrative انجام دهد:

CVE-2020-11896, CVE-2020-11897, CVE-2020-11898,
CVE-2020-11899, CVE-2020-11900, CVE-2020-11901,
CVE-2020-11902, CVE-2020-11903, CVE-2020-11904,
CVE-2020-11905, CVE-2020-11906, CVE-2020-11907,
CVE-2020-11908, CVE-2020-11909, CVE-2020-11910,
CVE-2020-11911, CVE-2020-11912, CVE-2020-11913,
(CVE-2020-11914 (Cisco Bug IDs: CSCvu68945

آسیب‌پذیری‌های موجود در اجرای Treck IP stack در مجموع با عنوان Ripple20 شناخته می‌شوند. اکسپلویت این مجموعه آسیب‌پذیری‌ها بسته به یک آسیب‌پذیری خاص، می‌تواند منجر به حملات اجرای کد از راه دور، انکار سرویس[3] یا افشای اطلاعات[4] شود. تیم واکنش به حوادث امنیتی سیسکو[5] اعلام کرده است که از هر گونه سوءاستفاده مخرب از این آسیب‌پذیری‌ها اطلاعی ندارد.

آسیب پذیری مذکور، تمام حالت‌های راه‌اندازی دستگاه‌های DCNM سیسکو که با

[1] validation
[2] insufficient authorization checking
[3] denial of service (DoS)
[4] information disclosure
[5] Cisco Product Security Incident Response Team (PSIRT)

استفاده از .ova و .iso installer نصب شده‌اند را تحت تاثیر قرار می‌دهد. نسخه‌های آسیب‌پذیر نرم‌افزار DCNM عبارتند از: 11.0(1)، 11.1(1)، 11.2(1) و 11.3(1).

با تایید شرکت سیسکو، آسیب‌پذیری ذکر شده نرم‌افزار DCNM را که با استفاده از DCNM installer برای سیستم‌عامل‌های ویندوز و لینوکس بر روی سیستم‌عامل‌های customer-provided نصب شده‌اند، تحت تاثیر قرار نمی‌دهد. این شرکت همچنین تایید کرده است که نسخه‌های x.7 و x.10 تحت تاثیر این آسیب‌پذیری قرار نمی‌گیرند.

سیسکو آسیب‌پذیری فوق را با انتشار نسخه 11.4(1) و بالاتر نرم‌افزار DCNM رفع و وصله کرده است. جهت دانلود این نرم‌افزار از Software Center در Cisco.com، مراحل زیر را دنبال کنید:

- بر روی Browse All کلیک کنید.
- Cloud and Systems Management > Data Center Infrastructure > Management > Data Center Network Manager را انتخاب کنید.
- از پنل سمت چپ Data Center Network Manager در این صفحه، یک نسخه را انتخاب کنید.

محصولات تحت تاثیر

به طور کلی این آسیب‌پذیری‌ها چندین محصول سیسکو را تحت تاثیر قرار می‌دهند که عبارتند از:

- IOS XE SD-WAN Software
- SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Cloud Routers
- SD-WAN vEdge Routers
- SD-WAN vManage Software
- SD-WAN vSmart Controller Software
- (DCNM software releases 11.0(1), 11.1(1), 11.2(1), and 11.3(1
- ASR 5000
- ASR 5500
- Virtual Packet Core
- StarOS Software

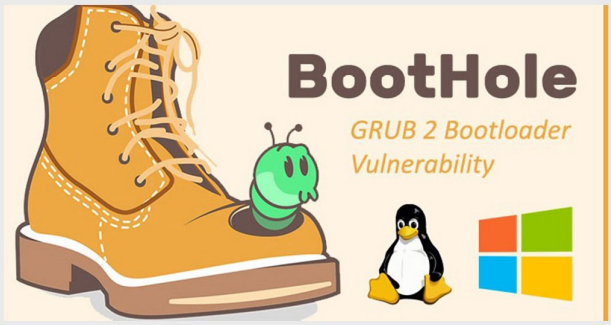
توصیه امنیتی

سیسکو چندین بروزرسانی نرم‌افزاری جهت رفع آسیب‌پذیری‌های بحرانی با شناسه‌های CVE-2020-3374، CVE-2020-3375 و CVE-2020-3382 و همچنین آسیب‌پذیری‌هایی با شدت بالا و متوسط را به صورت رایگان منتشر کرده است. CERT-EU به کاربران توصیه می‌کند با توجه به شدت و اهمیت آسیب‌پذیری‌های عنوان شده که در اسرع وقت نسبت اعمال به بروزرسانی‌های منتشر شده اقدام نمایند.

منبع خبر:

Scan Link

تحت تأثیر قرار گرفتن میلیاردها سیستم ویندوزی و لینوکسی توسط آسیب‌پذیری BootHole



این آسیب‌پذیری با شناسه CVE-2020-10713 و تحت عنوان BootHole، در بوت لودر[1] GRUB2 وجود دارد و مهاجمان در صورت بهره‌برداری موفق از این آسیب‌پذیری می‌توانند قابلیت Secure Boot را دور بزنند و سطح دسترسی بالایی به صورت مخفیانه و ماندگار در سیستم‌های هدف به دست آورند. قابلیت Secure Boot یک ویژگی امنیتی از (Unified Extensible Firmware Interface (UEFI است که از یک بوت‌لودر برای بارگیری اجزای حساس، وسایل جانبی و سیستم‌عامل استفاده می‌کند.

آسیب‌پذیری مذکور دارای شدت 8.2 از 10 بوده و در واقع یک آسیب‌پذیری سرریزبافر است که در GRUB2، هنگام تجزیه‌ی[2] فایل grub.cfg رخ می‌دهد و تمام نسخه‌های GRUB2 تحت تأثیر این آسیب‌پذیری قرار دارند. این فایل پیکربندی، یک فایل خارجی بوده و در پارتیشن سیستمی EFI قرار دارد، بنابراین می‌تواند توسط مهاجم دارای سطح دسترسی مدیر بدون تغییر در عملکرد بوت‌لودرِ GRUB2، تغییر داده شود. grub.cfg یک فایل متنی بوده و همانند سایر فایل‌ها یا فایل‌های اجرایی امضاء[3] نشده است. همین امر فرصت را برای مهاجمان فراهم می‌آورد تا مکانیسم hardware root of trust را بشکنند. در این حالت، بافر به جای متوقف کردن اجرا یا خارج شدن از فرآیند، فقط خطایی را در کنسول چاپ می‌کند و به فراخوانی تابع بازمی‌گردد. به گفته‌ی محققان، سرریز بافر به مهاجم اجازه می‌دهد امکان اجرای کد دلخواه را در محیط اجرایی UEFI به دست آورد، که این امر می‌تواند برای اجرای بدافزار، تغییر فرآیند بوت، وصله‌ی مستقیم هسته‌ی سیستم‌عامل و یا هر اقدام مخرب دیگری مورد سوءاستفاده قرار گیرد.

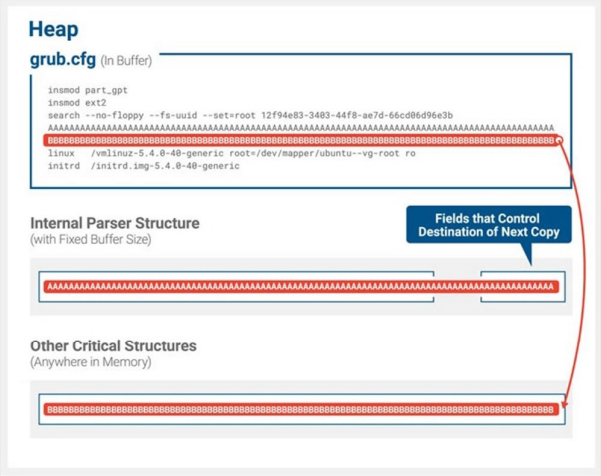
به منظور بهره‌برداری از آسیب‌پذیری BootHole در سیستم‌های ویندوزی، مهاجمان می توانند بوت‌لودرهایِ پیش‌فرضِ نصب شده بر روی سیستم را با یک نسخه آسیب‌پذیر GRUB2، جهت نصب بدافزار rootkit جایگزین کنند.

همانطور که در تصویر زیر قابل مشاهده است، محتوای grub.cfg از دیسک به بافر هیپ خوانده شده و سپس توسط کد آسیب‌پذیر تجزیه می‌شود که در نتیجه موجب سرریز ساختار تجزیه‌گر[4] داخلی می‌گردد.

سرریز بافر در ساختار تجزیه‌گر داخلی

[1] bootloader
[2] parse
[3] sign
[4] parser

همچنین مطابق آنچه در تصویر زیر آمده است، فیلدهای موجود در ساختار تجزیه‌گر داخلی بازنویسی شده و امکان نوشتن داده‌ی دلخواه در هر بخش از حافظه امکان‌پذیر می گردد.



بازنویسی فیلدهای تجزیه‌گر داخلی جهت نوشتن داده‌ی دلخواه

البته لازم به ذکر است که این آسیب‌پذیری از راه دور قابل بهره‌برداری نبوده و مهاجم باید پیش از هر چیز ابتدا راه نفوذی به سیستم هدف بیابد و بتواند سطح دسترسی خود را به Admin یا root ارتقاء دهد، تا بتواند از آسیب‌پذیری مذکور سوءاستفاده کند. از طرف دیگر مهاجم باید دسترسی فیزیکی به سیستم هدف داشته باشد.

نسخه‌های تحت تأثیر این آسیب‌پذیری

این آسیب‌پذیری میلیاردها دستگاه در سراسر جهان ـ از جمله سرورها و ایستگاه‌های کاری، لپ‌تاپ‌ها، دسکتاپ‌ها و سیستم‌های IoT و تقریباً هر سیستم لینوکسی و ویندوزی ـ را تحت تأثیر قرار می‌دهد. اگرچه GRUB2 یک بوت‌لودر استاندارد است که توسط اکثر سیستم‌های لینوکسی مورد استفاده قرار می‌گیرد، اما سیستم‌عامل‌های دیگر، هسته‌ها و هایپروایزرهایی نظیر XEN را نیز پشتیبانی می‌کند. همچنین این مشکل برای هر دستگاه ویندوزی که از Secure Boot با استاندارد Microsoft Third Party UEFI Certificate Authority استفاده می‌کند قابل تعمیم است.

راهکار

نظارت بر محتوای پارتیشن بوت‌لودر (پارتیشن سیستمی EFI) می‌تواند در شناسایی زودهنگام سیستم‌های آسیب‌دیده در سازمان کمک‌کننده باشد. راه‌حل های زیر جهت کاهش و رفع آسیب‌پذیری پیشنهاد می‌گردد:

- به‌روزرسانی GRUB2 جهت رفع آسیب‌پذیری.
- به‌روزرسانی bootloaders، installers و shims در تمام نسخه‌های لینوکس و سایر محصولاتی که از GRUB2 استفاده می‌کنند.
- امضاء shimsهای جدید توسط صادرکنندگان گواهی UEFI شخص ثالث مایکروسافت.
- نصب نسخه‌ی جدید سیستم‌عامل در دستگاه‌های آسیب‌پذیر.
- به‌روزرسانی لیست ابطال UEFI (dbx) در سیستم‌عامل دستگاه‌های آسیب‌پذیر جهت جلوگیری از اجرای کد هنگام بوت شدن سیستم.
- جایگزین نمودن بوت‌لودرهای جدید با بوت‌لودرهای قدیمی و ابطال بوت‌لودرهای قدیمی و آسیب‌پذیر جهت جلوگیری از سوءاستفاده مهاجمان.

[1] cleartext

منبع خبر :

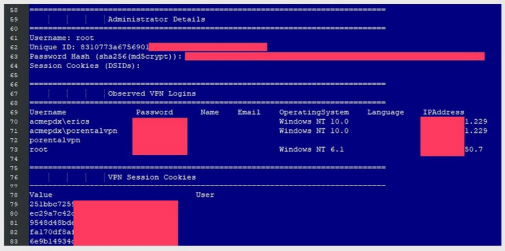
Scan Link

افشای رمزعبور بیش از 900 VPN سرور!

محققان امنیتی ابتدا در سال 2019 در خصوص یک آسیب‌پذیری که بر محصول VPN شرکت Pulse Secure تأثیر می‌گذارد هشدار دادند، این آسیب‌پذیری با شناسه "CVE-2019-11510" و Base Score 10 از 10 و شدت بحرانی، به مهاجمان اجازه خواهد داد تا از راه دور و به صورت غیرمجاز به شبکه شرکت‌ها متصل شوند، تأیید هویت چندعاملی را غیرفعال کنند و از راه دور لاگ‌ها و گذرواژه‌هایی با متن ساده، ازجمله گذرواژه‌های حساب کاربری Active Directory را مشاهده کنند؛ تا آن که در تاریخ 4 آگوست 2020 یک هکر، لیستی از آدرس IP بیش از 900 سرور Pulse Secure VPN و همچنین نام‌های کاربری و رمزهای عبوری که از الگویی ساده برای انتخاب کاراکترهای آن‌ها استفاده شده بود منتشر کرد که تحت تأثیر این آسیب‌پذیری بحرانی قرار گرفته‌اند.

کارشناسان امنیتی وبسایت ZDNet که نسخه‌ای از این لیست را با کمک شرکت اطلاعاتی KELA بدست آورده است نیز صحت این موضوع را تأیید می‌کنند. همانطور که در تصویر مشاهده می‌کنید و طبق بررسی‌های صورت گرفته، این لیست شامل موارد زیر می‌باشد:

- IP آدرس سرورهای Pulse Secure VPN
- سرور Pulse Secure VPN نسخه firmware
- کلیدهای SSH هر سرور
- لیستی از تمامی کاربران محلی و رمزهای عبور هش شده آن‌ها
- جزئیات حساب کاربری مدیر
- آخرین ورودهای VPN (شامل نام‌های کاربری و رمزهای عبوری که از الگویی ساده[1] برای انتخاب کاراکترهای آن‌ها استفاده شده است)
- کوکی‌های VPN session

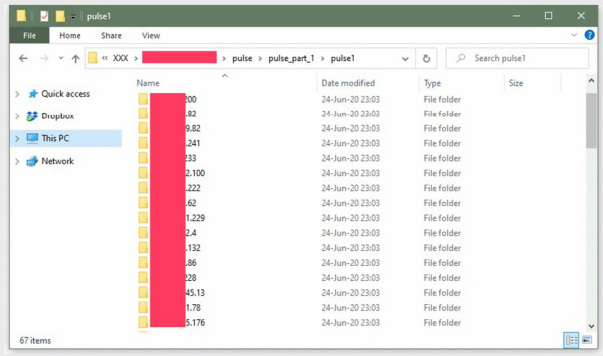


لیست اطلاعات فاش شده از VPN سرورها

جزئیات فنی و روش بهره‌برداری

با اکسپلویت این آسیب‌پذیری، مهاجم به سیستم‌ها دسترسی پیدا می‌کند، جزئیات سرور از جمله نام کاربری و رمزعبور را به سرقت می‌برد و در نهایت تمام اطلاعات را در یک منبع مرکزی ذخیره خواهد کرد.

بر اساس تصویر منتشر شده در وبسایت ZDNet، همانطور که در پوشه‌های موجود در شکل 2 مشاهده می‌کنید، تاریخ اسکن فضای آدرس IPv4 و یا لیست گردآوری شده از اطلاعات VPN سرورها مربوط به بازه زمانی 24 ژوئن تا 8 ژوئیه 2020 می‌باشند.



تاریخ اسکن فضای آدرس IPv4 و یا لیست گردآوری شده از اطلاعات VPN سرورها گفتنی است که از بین 913 آدرس IP منحصربفرد و پس از بررسی‌های صورت گرفته توسط اسکنرهای Bad Packets CTI، 677 مورد از این آدرس IPها در سال گذشته هنگام اکسپلوت عمومی این آسیب‌پذیری، نسبت به آن آسیب‌پذیر بوده‌اند؛ همچنین در بین لیست منتشر شده، مشخص شده است که 677 شرکت از نخستین اسکن Bad Packets در سال گذشته، هنوز وصله نشده‌اند؛ حتی اگر این شرکت‌ها سرورهای Pulse Secure خود را وصله کنند، جهت جلوگیری از سوءاستفاده هکرها، باید رمزهای عبور خود را تغییر دهند. لیست مذکور در یک تالارگفتگو در بین هکرها به اشتراک گذاشته شده است تا توسط باندهای مختلفی مانند REvil (Sodinokibi), NetWalker, Lockbit, Avaddon, Makop و Exorcist مورد سوءاستفاده قرار گیرد. بسیاری ازاین باندها با استفاده از سرورهای Pulse Secure VPN وارد شبکه‌های سازمانی شده و از قربانیان طلب باج خواهند کرد. نکته مهم آن است که سرورهای Pulse Secure VPN معمولاً به عنوان gateway دسترسی به شبکه‌های شرکتی، مورد استفاده قرار می گیرند تا کارکنان آن‌ها بتوانند از طریق اینترنت و از راه دور به اپلیکیشن‌های داخلی وصل شوند.

سرورهای تحت تأثیر

تحلیلگری به نام Bank Security و کسی که در همان لحظات اولیه از لیست مذکور اطلاع پیدا کرد و آن را با ZDNet به اشتراک گذاشت، نظر جالبی درخصوص این لیست و محتوای آن بیان نمود؛ به گفته وی، تمامی سرورهای Secure VPN موجود در لیست، نسخه‌ای از firmware را اجرا می‌کنند که نسبت به این نقص آسیب‌پذیر هستند؛ وی معتقد است هکری که این لیست را منتشر کرده است، تمامی فضای آدرس IPv4 اینترنت را برای سرورهای Pulse Secure VPN اسکن کرده است.

توصیه امنیتی

برای مقابله با این آسیب‌پذیری و جلوگیری از تحت تأثیر قرار گرفتن سرورها، هر چه سریع تر وصله‌های امنیتی منتشر شده توسط Pulse Secure را اعمال کنید و اگر سازمان شما از Pulse Connect Secure استفاده می‌کند، در اسرع وقت نسبت به اعمال وصله امنیتی منتشر شده اقدام کنید.

منبع خبر :

Scan Link

اخبار کوتاه

باگ امنیتی ویندوز امکان نفوذ به پرینتر را فراهم می‌کند

اخیراً یک باگ امنیتی در ویندوز شناسایی شده که روی پرینتر تاثیر می‌گذارد. مایکروسافت اعلام کرده که با انتشار یک پچ امنیتی این مشکل را برطرف خواهد کرد. محققان توانسته‌اند پچ‌های امنیتی را دور بزنند و از این باگ سوءاستفاده کنند که نتیجه آن، امکان نفوذ به هر یک از دستگاه‌های پرینت و کنترل شبکه خصوصی می‌شود. این نقص امنیتی روی «Print Spooler» ویندوز تاثیر می‌گذارد، سرویسی که فرآیند پرینت کردن را مدیریت می‌کند. افراد می‌توانند از این آسیب‌پذیری برای اجرای بدافزار استفاده کنند.

این آسیب‌پذیری که با شناسه «CVE-2020-1048» شناخته می‌شود، به مایکروسافت اطلاع داده شد و این غول نرم‌افزاری نزدیک به سه ماه پیش برای آن پچ منتشر کرد، با این حال به نظر می‌رسد این مشکل به صورت کامل رفع نشده است. محققان به این موضوع پی بردند که می‌توانند از CVE-2020-1048 برای ایجاد فایل های مخرب استفاده کنند. از جمله این فایل‌ها می‌توان به SHD اشاره کرد که حاوی متادیتا برای کارهای پرینتر مانند آی‌دی سیستم کاربر و فایل‌های SPL حاوی اطلاعاتی مورد نیاز برای پرینت است.

هکرها تا انتشار آپدیت مایکروسافت می‌توانند به شبکه‌های پرینت حمله کنند و علاوه بر این، بسیاری از کاربران پچ‌های اولیه مایکروسافت را دانلود نمی‌کنند و منتظر بروزرسانی های بعدی باقی می‌مانند چرا که این آپدیت‌ها خود می‌توانند حاوی باگ باشند.

مقالات آموزشی

فعال سازی Audit Log در سیستم

Event Log

همانطور که از اسم این سرویس نیز بر می‌آید سرویس Windows Event Log یا همان EventLog در ویندوز برای گزارش یا Log برداری از رویداد یا Event های اتفاق افتاده در سیستم، اجزای سیستمی و نرم‌افزارها مورد استفاده قرار می‌گیرد. این سرویس مهم و حیاتی در ویندوز توابعی را ارائه می‌دهد که به برنامه‌ها این امکان را می‌دهد تا Log ها را مدیریت و نگهداری کنند و همچنین عملیاتی نظیر آرشیو سازی و پاکسازی را روی Log ها انجام دهند.

با استفاده از این سرویس مدیران سیستم می‌توانند Logها را نگهداری کنند و وظایف مدیریتی را با توجه به سطح دسترسی‌شان انجام دهند. سرویس Windows Event Log می‌تواند Log ها را مدیریت، آرشیو، نگهداری و همچنین پاکسازی کند. این سرویس همچنین امکان نمایش Logها را هم با فرمت XML و هم با فرمت Plain Text به ما می‌دهد.

فعال کردن Security Audit Policy

به منظور فعال کردن Security Audit Policy در سیستم بایستی مراحل ذیل را انجام دهید.

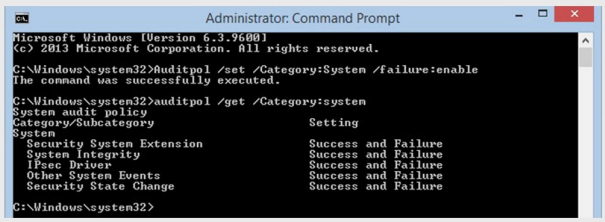
1- برای باز کردن پنجره Command Prompt روی میانبر Cmd.exe بر روی دسکتاپ کلیک و سپس گزینه Run as administrator را انتخاب کنید.

2- دستور زیر را در پنجره Command Prompt واردکنید.

```
Auditpol /set /Category:System /failure:enable
```

3- سیستم را یک بار Restart کنید تا تغییرات اعمال شود.

تصویر (1) نحوه فعال‌سازی Auditpolرا نشان می‌دهد.



تصویر(1)

نحوه ورود به سیستم و تشخیص رویدادها از طریق فعال کردن Code Integrity

برای فعال کردن ورود به سیستم ، مراحل زیر را انجام دهید:

1- پنجره Cmmand Prompt را با کنید.

2- در خط فرمان Eventvwr.exe را اجرا کنید.

3- در سمت چپ صفحه Event Viewer زیر پوشه‌های زیر را باز کنید.

a. Applications and Service Logs

b. Microsoft

c. Windows

-4بسط مربوط به Windows را باز و زیر پوشه Code Integrity را انتخاب کنید.

-5 در سمت راست گزینه View را انتخاب کنید.

-6 گزینه Show Analytic and Debug Logs را انتخاب کنید . سپس در Event Viewer زیر پوشه Operational و پوشه Verbose را انتخاب کنید.

-7 روی Verbose کلیک راست کرده سپس از منو نمایش داده شده Properties را انتخاب کنید.

-8 در پنجره باز شده از بخش General گزینه Properties و سپس گزینه Enable را انتخاب کنید.

-9 پس از انجام مراحل فوق به منظور اعمال تغییرات، سیستم را یک بار Restart کنید.

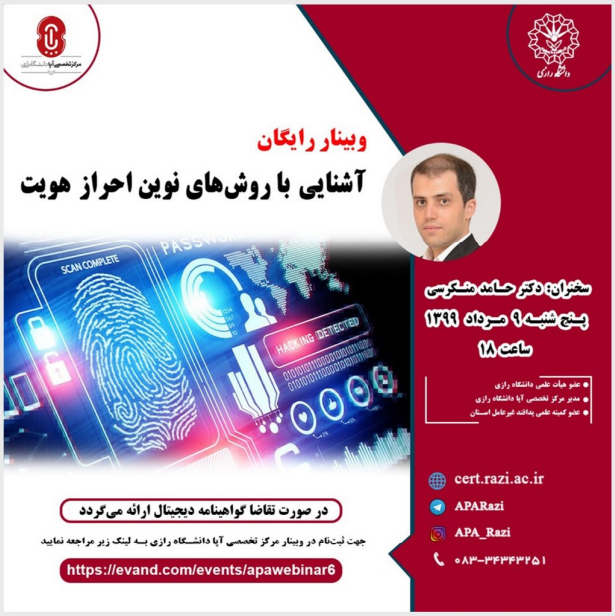
اخبار داخلی

وبینار رایگان آشنایی با روش‌های نوین اح راز هویت

گسترش زیر ساخت فناوری اطلاعات سازمانهای بزرگ و پیشرو بر تعدد سامانههای آن ها میافزایند. در روند گسترش سامانهها هریک از آنها بصورت جزیرهای جدا و مستقل از دیگر سامانهها ایجاد میگردند. کاربران برای دسترسی به هر سامانه نیازمند نگهداری و استفاده از یک هویت دیجیتال مجزا میباشند. تکرار اطلاعات هویت هر کاربر در سامانههای جزیره ای جدا از یکدیگر به مرور، استفاده کاربران از سامانهها و همچنین مدیریت کاربران توسط مدیران این سامانهها را بسیار دشوار و پر خطا میسازد. مشکل بودن بخاطر سپردن نام کاربری و کلمه عبور، باعث میگردد بسیاری از کاربران از کلمات عبور سادهتر استفاده کنند و یا کلمه عبور خود را در دسترس خود روی میز کارشان قرار دهند، که این مسئله سامانهها را بسیار نا امن ساخته و میتواند کسب و کار آن سازمان را دچار مخاطره نماید. به طور کلی معماری سنتی سامانههای گسسته و جزیرهای، باعث عدم امکان کنترل و نظارت متمرکز بر مدیریت کاربران، احراز هویت آنها و کنترل دسترسی آنها به بخشهای مختلف سامانههای گوناگون سازمان میگردد، که این ضعف به سادگی میتواند کسب و کار سازمان را دچار مخاطرات جدی نماید.

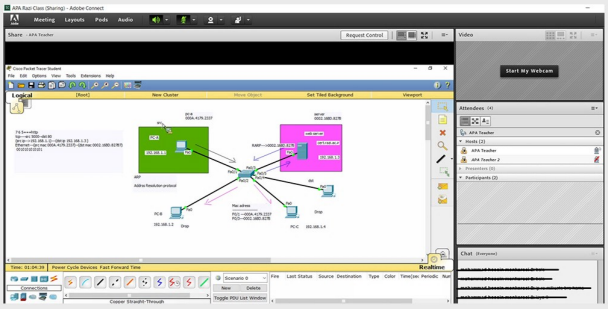
بطور مثال عدم وجود کنترل و شفافیت کافی در مدیریت کاربران باعث میگردد، هنگام خروج یک فرد از سازمان، کاربران در سیستمهای متعدد و گوناگون آن سازمان، حتی بعد از چندین ماه یا سال فعال بوده و به منابع اطلاعاتی سازمان دسترسی داشته باشد و یا بر عکس به هنگام اضافه شدن یک فرد به سازمان، ایجاد هویت دیجیتال برای او نیازمند درگیر شدن مدیران سیستمهای گوناگون مرتبط باشد که طبیعتاً نمیتوانند به موقع و موثر کاربر آن فرد جدید را در همه سیستمهای مورد نیاز ایجاد و دسترسیهای مربوطه را پیکربندی کنند، همچنین هیچ گونه سابقهای از صدور کاربر و تغییر دسترسیها چه به اشتباه و چه غیر قانونی وجود نخواهد داشت. بدیهی است چنین شرایطی بهرهوری و امنیت استفاده کاربران از سیستمهای نرمافزاری که عملا کسب و کار سازمان را تشکیل میدهند، دچار مشکلات جدی میسازد.

ویت کاربران برای استفاده تمامی سامانههای نرمافزاری و سرویسهای سازمانی برای بانکها و موسسات مالی و اعتباری امری ضروری و ناگزیر است. در همین راستا با توجه مشکلات ذکر شده.، به منظور آشنایی علاقمندان این حوزه در مورخ 9 مرداد ماه 1399 وبینار رایگان آشنایی با روشهای نوین احراز هویت با استقبال پرسنل سازمانها، شرکت های خصوصی، دانشجویان و علاقمندان توسط مرکز آپا برگزار گردید.

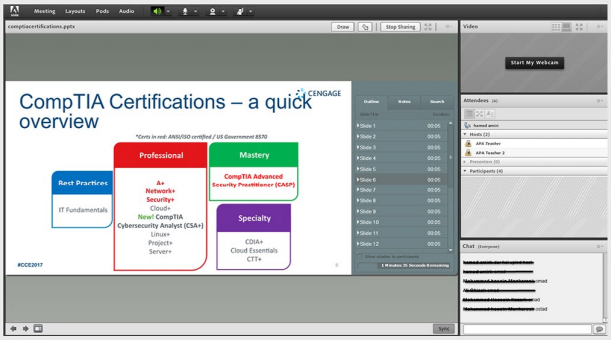


شروع دوره های جدید آنلاین

شروع دوره مقدماتی شبکه Network+ مرکز تخصصی آپا دانشگاه رازی به صورت آنلاین برای دانجشویان و علاقمندان به منظور ورود به حوزههای تخصصی فناوری اطلاعات، در تاریخ 13 مرداد ماه به مدت 40 ساعت با تدریس خانم مهندس آرزو حسنی در حال برگزاری می باشد.



شروع دوره مقدماتی امنیت شبکه Security+ مرکز تخصصی آپا دانشگاه رازی به صورت آنلاین برای دانجشویان و علاقمندان به منظور ورود به دنیای امنیت اطلاعات سایبری، در تاریخ 12 مرداد ماه به مدت 40 ساعت با تدریس آقای مهندس مهدی فرهمند در حال برگزاری می باشد.



اخبار کوتاه

FBI مدعی حمله هکرهای ایرانی به تجهیزات شبکه F5 شد

FBI اخیرا ادعا کرده گروهی از هکرهای منتسب به ایران به بخش‌های خصوصی و دولتی ایالات متحده آمریکا حمله کرده‌اند. در حالی FBI چنین ادعایی را مطرح کرده که نام این هکرهای ایرانی را مشخص نکرده، البته منابع به اسم رمز این گروه، «Fox Kitten» یا «Parasite» اشاره کرده‌اند. این گروه هکری برای دستیابی به اهداف خود، به تجهیزات شبکه گران قیمت حمله می‌کند و برای این کار به سراغ آسیب‌پذیری‌های جدید می‌رود و پیش از اینکه شرکت‌ها بتوانند آن‌ها را برطرف کنند، به دستگاه‌ها دسترسی پیدا می‌کند. این دستگاه‌ها در شبکه‌های دولتی و خصوصی بزرگ مورد استفاده قرار می‌گیرند. به گفته این تحلیلگر، وظیفه اصلی این گروه مهیا کردن شرایط برای حملات گروه‌های دیگر مانند «Shamoon» و «Oilrig» است.

زمانی که هکرها به دستگاه دسترسی پیدا کنند، روی آن در پشتی یا بک دور ایجاد کرده و تجهیزات را وارد شبکه هک شده می‌کنند. طبق گزارش‌هایی که اوایل سال جاری میلادی توسط دو شرکت امنیت سایبری منتشر شد، این گروه هکری از تابستان سال گذشته با چنین روشی از آسیب‌پذیری‌ها سوءاستفاده کرده و دستگاه‌های VPNهای Pulse Secure، سرورهای Fortinet VPN با سیستم‌عامل FortiOS، سرورهای VPN محافظت جهانی Palo Alto Networksرا مورد حمله قرار داده‌اند.

زمانی که هکرها به دستگاه دسترسی پیدا کنند، روی آن در پشتی یا بک دور ایجاد کرده و تجهیزات را وارد شبکه هک شده می‌کنند. طبق گزارش‌هایی که اوایل سال جاری میلادی توسط دو شرکت امنیت سایبری منتشر شد، این گروه هکری از تابستان سال گذشته با چنین روشی از آسیب‌پذیری‌ها سوءاستفاده کرده و دستگاه‌های VPNهای Pulse Secure، سرورهای Fortinet VPN با سیستم‌عامل FortiOS، سرورهای VPN محافظت جهانی Palo Alto Networksرا مورد حمله قرار داده‌اند.

خطر هک در کمین یک میلیارد موبایل؛ چندین آسیب‌پذیری در چیپ‌های کوالکام کشف شد

محققان امنیتی موفق به کشف چندین آسیب‌پذیری جدید در چیپ‌های اسنپدراگون کوالکام شده‌اند که می‌توانند خطرات جدی برای کاربران به همراه داشته باشند.در گزارشی که اخیراً توسط Check Point منتشر شده، پژوهشگران بیش از 400 آسیب پذیری در پردازشگر سیگنال دیجیتال (DSP) چیپ‌های اسنپدراگون کوالکام را شناسایی کرده‌اند که در صورت سوءاستفاده از آن‌ها، هکرها می‌توانند کنترل بیش از 40 درصد تمام گوشی‌های هوشمند جهان را در اختیار بگیرند.

آسیب‌پذیری‌های کشف شده، تاثیر جدی روی اکثر گوشی‌های هوشمند موجود در بازار مجهز به چیپ‌های اسنپدراگون شامل پرچمدارهای شرکت‌های گوگل، سامسونگ، ال جی، شیائومی، وان پلاس و دیگر برندها دارد. هکرها با سوءاستفاده از این آسیب‌پذیری‌ها در DSP کوالکام می‌توانند از کاربران جاسوسی کنند و با ایجاد یک بدافزار غیرقابل حذف، مانع از شناسایی شوند. Check Point یافته‌های خود را در اختیار کوالکام قرار داده، این شرکت چنین موضوعی را تایید کرده و به سازندگان نیز اطلاع داده است. هم اکنون کوالکام پچ 6 مشکل امنیتی را منتشر کرده، اما سازندگان گوشی‌های هوشمند باید آن را در اختیار کاربران قرار دهند که با توجه به این موضوع، هنوز بسیاری از دستگاه‌ها در معرض خطر قرار دارند.

کوالکام در بیانیه‌ای اعلام کرده که حفظ امنیت کاربران یکی از اولویت‌های اصلی این کمپانی است و همچنین مدرکی مبنی بر سوءاستفاده از این آسیب‌پذیری‌ها وجود ندارد. این شرکت کاربران را ترغیب به نصب پچ‌ها از محل‌های قابل اعتماد مانند گوگل پلی استور کرده است. با توجه به شدت آسیب‌پذیری، به تمام کاربران پیشنهاد می‌شود که در صورت دریافت هرگونه پچ امنیتی، آن را روی دستگاه خود نصب کنند.

مرکز تخصصی آپا دانشگاه رازی