# بولتن خبری مرکز تخصصی آپا

کرمانشاه/دانشگاه رازی/شماره اول/تیرماه۱۳۹۷

مرکز تخصصی آپا دانشگاه رازی
پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

## ویژگی ضد جعل جدید در اندروید برای ایجاد امنیت از طریق احراز هویت بیومتریک

گوگل اعلام نمود ویژگی ضد جعل جدیدی به سیستم عامل اندروید خود افزوده است که به وسیله آن مکانیزم های احراز هویت بیومتریک این سیستم عامل را ایمن تر از قبل میکند. مکانیزم های بیومتریک شامل: اثر انگشت، تشخیص عنبیه، فناوری تشخیص چهره و غیره می باشند، که توسط آنها...

۳ گروه خبر : اخبار امنیتی

## کشف باگ حیاتی در مرورگرهای مدرن

محققان گوگل آسیب پذیری حیاتی جدیدی در مرورگرهای وب کشف نموده اند، که به موجب آن مرورگر وب می تواند به وب سایتی که شما از آن بازدید کرده اید اجازه دهد اطلاعات حساب کاربری که در وب سایت دیگری بر روی همان مرورگر وارد...

گروه خبر : آسیب پذیری ۱۱

## حل مشکل نصب برنامه های اندروید از منابع ناشناس توسط گوگل

آیا تعجب می‌کنید که چگونه آخرین آپدیت‌های مربوط به یک برنامه اندرویدی _که از طریق یک منبع ناشناس ثالث یا از طریق اشتراک‌گذاری نظیر به نظیر نصب شده است_ مستقیماً از طریق Google Play Store دریافت می‌گردد؟

به دلایل امنیتی، تا کنون برنامه‌های نصب شده از منابع شخص ثالث نمی‌توانستند به طور خودکار به روزرسانی شوند، زیرا ...

٦ گروه خبر : اخبار امنیتی

## هزاران برنامه تلفن همراه پایگاه داده Firebase محافظت نشده خود را افشاء میکنند.

محققان امنیتی موبایل، پایگاه داده های Firebase حفاظت نشده ای از هزاران برنامه iOS و اندروید کشف ...

۸ گروه خبر : اخبار امنیتی

## ده ها آسیب پذیری مهم و حیاتی در طیف وسیعی از محصولات سیسکو

کشف اسیب پذیری حیاتی در یکی از دستگاههای مدیریت دسترسی سیسکو این امکان را به هکرها می دهد که از راه دور به شبکه شرکت های بزرگ ...

۱۳ گروه خبر : آسیب پذیری


مرکز تخصصی آپادانشگاه رازی
کرمانشاه، طاق بستان، دانشگاه رازی،
ساختمان کتابخانه مرکزی، طبقه دوم، مرکز تخصصی آپا
apa@razi.ac.ir
۰۸۳۳۴۲۷۳۳۹۰
www.cert.razi.ac.ir

مرکز تخصصی آپا دانشگاه رازی

# هوالعلیم

## سخن سردبیر

بدون شک، در دنیای امروز که با سرعت هر چه تمام‌تر به سمت فناوری های نوین پیش می‌رود، آگاهی از مخاطرات و تهدیدات امنیتی پیش روی این پیشرفت امری مهم و حائز اهمیت بوده و افزایش دانش و آگاهی در این زمینه را می‌طلبد. اکنون با توجه به این امر مهم و نیز رسالت مرکز آپا در آگاهی‌رسانی، پشتیبانی و امداد در حوزه امنیت سایبری، برآن شدیم تا گامی دیگر در جهت رسالت خود در زمینه آگاهی‌رسانی به کاربران دنیای گسترده فناوری اطلاعات برداریم و بولتن خبری خود را تحت عنوان "بولتن خبری مرکز تخصصی آپا دانشگاه رازی" منتشر نماییم.

بولتن خبری این مرکز شامل فصل‌های گوناگونی در رابطه با اخبار و مقالات امنیتی بوده که عناوین آن به شرح ذیل آمده است:

- اخبار امنیتی: شامل جدیدترین اخبار امنیتی در یک ماه گذشته می باشد.
- آسیب‌پذیری: شامل مهمترین آسیب پذیریهای کشف شده در ماه گذشته می باشد.
- مقالات آموزشی: در هر شماره به ارائه نکات آموزشی در خصوص ابزارهای مرتبط به امنیت اطلاعات خواهیم پرداخت.
- امنیت کاربر رایانه: در هر شماره توصیه های مفید و کاربردی در جهت افزایش دانش کاربران در زمینه استفاده امن از رایانه شخصی و سازمانی ارائه خواهد شد.

به اطلاع علاقمندان حوزه امنیت سایبری و همراهان همیشگی می‌رسانیم که با همت و تلاش همکاران ما در این مرکز، از این پس بولتن خبری مرکز تخصصی آپا دانشگاه رازی در تاریخ پانزدهم هر ماه منتشر می‌گردد. علاقمندان می توانند به نسخه دیجیتالی این بولتن از طریق پایگاه اینترنتی و سایر کانالهای ارتباطی مرکز دسترسی داشته باشند. در صورت نیاز به نسخه مکتوب می توانید با همکاران ما در مرکز تماس بگیرید.

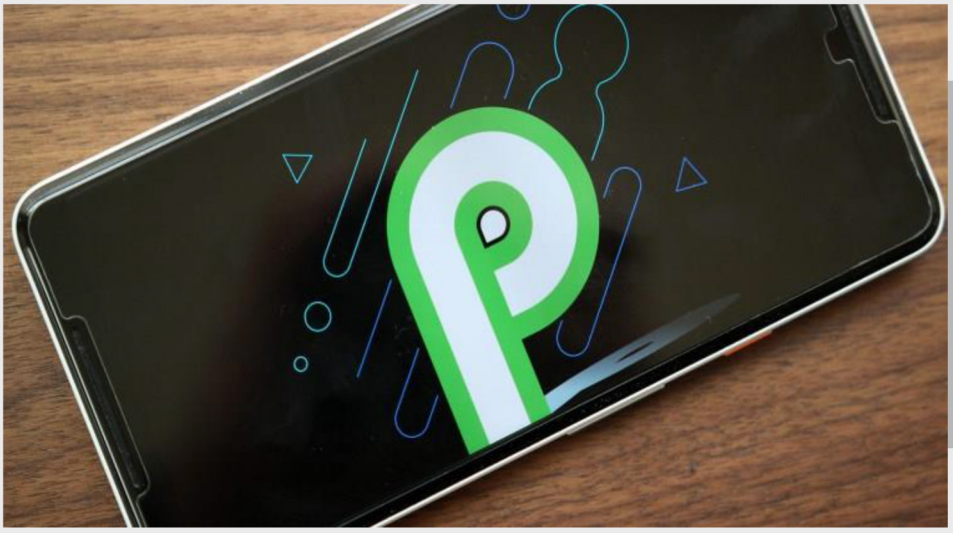
منتظر شنیدن خبرهای داغ امنیتی و توصیه های مفید در این بولتن خبری باشید.

# اخبار امنیتی

# ۱. ویژگی ضد جعل جدید در اندروید برای ایجاد امنیت از طریق احراز هویت بیومتریک

اخبار امنیتی (گردآورنده: مرضیه حسینی)

گوگل اعلام نمود ویژگی ضد جعل جدیدی به سیستم عامل اندروید خود افزوده است که به وسیله آن مکانیزم های احراز هویت بیومتریک این سیستم عامل را ایمن تر از قبل می کند. مکانیزم های بیومتریک شامل: اثر انگشت، تشخیص عنبیه، فناوری تشخیص چهره و غیره می باشند، که توسط آنها فرآیند بازگشایی قفل دستگاه ها و برنامه ها بسیار سریعتر و ایمن تر می گردد.



با این وجود، مشکلات سیستم های بیومتریک بر کسی پوشیده نیست، چرا که پیش از این چندین بار آسیب پذیر بودن اسکنرهای بیومتریک در مقابل حملات جعل اثبات شده است و در اغلب موارد ، توانسته اند آن ها را به راحتی فریب دهند.

## معیارهای جدید بیومتریک برای شناسایی حملات جعل

در حال حاضر سیستم احراز هویت بیومتریک اندروید از دو مکانیزم False Accept Rate (FAR) و False Reject Rate(FRR)، در ترکیب با تکنیک‌های یادگیری ماشین (machine learning) استفاده می‌کنند که برای اندازه‌گیری دقت و صحت ورودی‌های کاربر به کار می‌روند.

به طور خلاصه، False Accept Rate مشخص می‌کند که مدل بیومتریک چگونه یک کاربر جعلی را به عنوان کاربر اصلی تشخیص می‌دهد، و در مقابل، False Reject Rate نشان می‌دهد که مدل بیومتریک چگونه ویژگی‌های بیومتریک کاربر اصلی را اشتباه شناسایی می‌کند.

علاوه بر این، برخی از اسکنرهای بیومتریک برای راحتی کاربران امکان احراز هویت موفقیت‌آمیز با نرخ اشتباه بالا را فراهم می‌کنند که این مسئله راه را برای حملات جعل روی دستگاه باز می‌کند.

گوگل می‌گوید: هیچ یک از ویژگی‌های بیومتریک، به اندازه کافی دقیق و صحیح نیستند که مانع از تلاش هکر برای دسترسی غیر مجاز به دستگاه از طریق حملات جعل شوند. برای حل این مسئله، علاوه بر FAR و FRR گوگل دو مکانیزم جدید را به قابلیت‌های پیشین اضافه کرده است. قابلیت‌های Spoof Accept Rate (SAR) و Imposter Accept Rate (IAR) که برای هکر یک تهدید به حساب می‌آیند.

Vishwath Mohanمهندس امنیتی تیم اندروید گوگل می‌گوید: "همان‌طور که از نام این ویژگی‌ها پیداست، این معیارها مشخص می‌کنند که چگونه یک هکر می‌تواند احراز هویت بیومتریک را دور بزند."

هکری که از روش جعل استفاده می‌کند می‌تواند از راه‌های مختلفی به هدف خود دست یازد، از جمله اینکه: می‌تواند صدای کاربر اصلی را ضبط نموده و برای احراز هویت آن را برای دستگاه پخش کند، عکس اثر انگشت یا چهره کاربر اصلی را برای ورود به دستگاه استفاده کند و غیره.

## اجرای سیاست‌های احراز هویت بیومتریک قوی برای گوگل

بر اساس ورودی بیومتریکی که کاربر انتخاب می‌کند، مقادیر SAR و IAR تعیین می‌کنند که آیا احراز هویت قوی است ( مقادیر کمتر یا مساوی ۷٪) یا ضعیف ( برای مقادیر بالاتر از ۷٪).

اگر برای باز کردن دستگاه یا برنامه‌ای از مقادیر بیومتریک ضعیف استفاده شود، Android P سیاست‌های سخت‌گیرانه ای را برای کاربر اعمال خواهد کرد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

- در صورتی که دستگاه حداقل ٤ ساعت غیر فعال باشد، مانند زمانی که در حال شارژ است، کاربر برای ورود باید رمز عبور، الگوی ورودی، پین کد اولیه، پسورد یا ویژگی بیومتریک قوی را دوباره وارد کند.
- اگر دستگاه برای ۷۲ ساعت بدون فعالیت باشد، سیستم از شما می‌خواهد مکانیزم‌های ذکر شده در بالا را هم برای بیومتریک ضعیف و هم برای بیومتریک قوی وارد کنید.
- برای افزایش ایمنی، کاربرانی که بیومتریک ضعیف استفاده می‌کنند امکان انجام تراکنش‌ها و پرداخت‌هایی که با KeyStore انجام می‌شود را ندارند.

علاوه بر این‌ها، گوگل یک BiometricPrompt API برای استفاده ساده توسعه‌دهندگان فراهم نموده است تا بتوانند از ویژگی‌های بیومتریک به منظور افزایش امنیت کاربران، در برنامه‌های خود بهره ببرند. با استفاده از این ویژگی، بیومتریک ضعیف از طریق دو مکانیزم جدید تشخیص داده شده و کاملاً غیرفعال می‌شود.

Mohan می‌گوید: "BiometricPrompt تنها بیومتریک‌های قوی را می‌پذیرد و یک توسعه دهنده با استفاده از آن می‌تواند مطمئن باشد که سطح امنیتی پایداری را در تمام دستگاه‌هایی که برنامه‌های خود را روی آن‌ها اجرا می‌کند، فراهم نموده است."

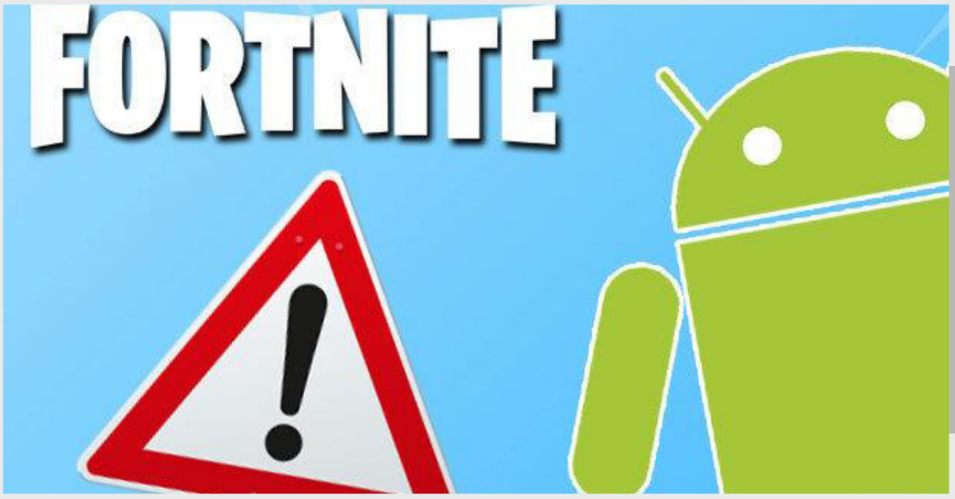
"یک کتابخانه پشتیبانی نیز برای دستگاه های دارای Android O و قبل از آن ارائه شده است، که به برنامه‌ها امکان می دهد از مزایای این API در بیشتر دستگاه‌ها استفاده کنند."

https://thehackernews.com/۲۰۱۸/۰٦/android-biometric-authentication.html

# ۲. نسخه های تقلبی بازی معروف فورتنایت اندروید

اخبار امنیتی (گردآورنده: محمد جلیلی)

هنوز نسخه سیستم عامل اندروید بازی فورتنایت موبایل منتشر نشده است اما نسخه های جعلی آن که اکثراً حاوی بدافزار هستند، به صورت گسترده ای در سطح اینترنت پخش شده اند.




از آن جایی که گوگل جلوی انتشار اپلیکیشن های تقلبی روی پلی استور را می گیرد، بسیاری از این نسخه های جعلی، از طریق ویدیویی در یوتیوب معرفی می شوند تا کسانی را که به دنبال نسخه اندروید این بازی هستند را به سمت دانلود فایل های مخربی سوق دهند.

متاسفانه این اپلیکیشن ها معمولاً ظاهری شبیه به نسخه ای او اس بازی دارند و حتی در اهنگام اجرای آن ها، نام اپیک گیمز و صفحه لودینگ اصلی فورتنایت را هم خواهید دید. بعد از پایان لودینگ، صفحه عجیبی به نمایش در خواهد آمد که یک «به روزرسانی جدید» برای بازی را به اطلاع شما خواهد رساند.

کلاهبرداری از همین جا شروع می شود، بعد از باز کردن صفحه این آپدیت، این اپلیکیشن تقلبی به شما اطلاع می دهد که برای ادامه کار نیاز به تایید تلفن همراه دارید و بعد از آن به صفحه ای هدایت می شوید که ربات نبودن شما را چک می کند، اما در واقع بعد از باز کردن آن، دانلود اپلیکیشن دیگری آغاز می شود.

به نظر می رسد خود این اپلیکیشن هایی که کاربر به اجبار آن ها را دانلود کرده، مخرب نیستند ولی فریب دادن کاربران به دانلود اپلیکیشنی که آن را نمی خواهند، آن هم با فورتنایتی که به هیچ عنوان فابل بازی نیست، کلاهبرداری محسوب می شود.

بسیاری از افرادی که این نوع برنامه ها را نصب می کنند، سن و سال کمی دارند و با ساز و کار این نوع کلاهبرداری ها آشنا نیستند. بنابراین بهتر است در صورت دیدن اپ فورتنایت روی تلفن همراه اندرویدی خود یا فرزندتان، برای جلوگیری از سو استفاده های احتمالی بعدی، آن را پاک کنید.

منبع خبر :

https://www.independent.co.uk/life-style/gadgets-and-tech/gaming/fortnite-android-apk-download-google-play-store-fake-virus-a٨٤٠٨٧٢١.html

https://bit.ly/٢lLnTgg

## ۳. حل مشکل نصب برنامه‌های اندروید از منابع ناشناس توسط گوگل

اخبار امنیتی (گردآورنده: پروین زنگنه)

آیا تعجب می‌کنید که چگونه آخرین آپدیت‌های مربوط به یک برنامه اندرویدی _که از طریق یک منبع ناشناس ثالث یا از طریق اشتراک‌گذاری نظیر به نظیر نصب شده است_ مستقیماً از طریق Google Play Store دریافت می‌گردد؟


به دلایل امنیتی، تا کنون برنامه‌های نصب شده از منابع شخص ثالث نمی‌توانستند به طور خودکار به روزرسانی شوند، زیرا گوگل آن‌ها را به عنوان برنامه‌های Google Play Store تشخیص نمی‌داد و در لیست برنامه‌های حساب کاربری گوگل نیز نمایش داده نمی‌شدند.

در اواخر سال گذشته، گوگل برنامه خود را برای ایجاد یک مکانیزم خودکار در تأیید صحت برنامه‌ها با اضافه کردن تعدادی مِتادیتا (metadata) امنیتی در بالای هر بسته نرم افزاری Android (در بلوک امضای APK) که توسط خودِ فروشگاه Play توزیع شده است اعلام کرد.

این متادیتا مانند یک امضای دیجیتالی است که به دستگاه Android شما کمک می‌کند تا تأیید کند که آیا برنامه ای که از یک منبع شخص ثالث نصب شده است، برنامه فروشگاه Play است یا خیر، به عنوان مثال، آیا ویروسی به آن پیوست نشده است.

از اوایل سال ۲۰۱۸، گوگل اجرای این مکانیسم را آغاز کرده است، که نیازمند هیچ اقدامی از جانب کاربران یا توسعه‌دهندگان برنامه‌های کاربردی Android نبوده و به این شرکت کمک می‌کند تا کاربران، تلفن‌های هوشمند خود را با اضافه کردن این برنامه‌های به اشتراک گذاشته شده در Play Store، طور منظم به روز رسانی کنند.

علاوه بر این، گوگل چند روز گذشته با افزودن پشتیبانی آفلاین برای تأیید متادیتا، یک پیشرفت جدید از برنامه خود اعلام کرد که به سیستم عامل Android شما اجازه می‌دهد تا اعتبار "برنامه‌های دانلود شده از طریق کانال‌های توزیع Play-approved " را تعیین کند ، این در حالیست که دستگاه آفلاین است.

James Bender مدیر محصول در google play بیان کرد:

"یکی از دلایلی که ما در حال انجام این کار هستیم این است که به توسعه‌دهندگان برای جذب مخاطبان بیشتر کمک کنیم، به ویژه در کشورهایی که به اشتراک‌گذاری نظیر به نظیر برنامه به دلیل هزینه بالای برنامه‌ها و اتصالات محدود، رایج‌تر است".

لازم به ذکر است که این ویژگی شما را از تهدید نصب برنامه‌ها از منابع شخص ثالث محافظت نمی‌کند بلکه صرفاً به شما کمک می‌کند که اگر منشأ برنامه‌های نصب شده دستگاه شما فروشگاه Google Play است بتوانید آخرین به روز رسانی برنامه‌ها را دریافت کنید.

گوگل همچنین به عنوان بخشی از مأموریت خود برای محافظت از سیستم Android، برنامه‌ای به نام Google Play Protect را اضافه کرد، که با استفاده از مکانیسم یادگیری ماشین و تجزیه و تحلیل، برنامه‌های خطرناک و مخرب را از بین می‌برد.

Google Play Protect نه تنها برنامه‌های نصب شده از Play Store را اسکن می‌کند، بلکه برنامه‌هایی که از منابع شخص ثالث نصب شده‌اند را نیز مورد بررسی قرار می‌دهد.

علاوه بر این، Play Protect هم اکنون از اسکن آفلاین نیز پشتیبانی می‌کند.

اگرچه فروشگاه Play به طور کامل مصون از بدافزارها نیست، اما برای به حداقل رساندن خطر ابتلا به بدافزارها هنوز هم به کاربران توصیه می‌شود که برنامه‌ها را از فروشگاه‌های رسمی برنامه، مانند Google play store، دانلود نمایند.

لینک خبر:

https://thehackernews.com/۲۰۱۸/۰۶/google-play-store-app-updates.html

# ۴. هزاران برنامه تلفن همراه پایگاه داده Firebase محافظت نشده خود را افشاء می‌کنند!

اخبار امنیتی (گردآورنده: پروین زنگنه)

محققـان امنیتـی موبایل، پایگاه داده‌های Firebase حفاظت نشـده‌ای از هزاران برنامه iOS و اندروید کشـف نموده‌اند که بیـش از ۱۰۰ میلیـون رکـورد داده، از جملـه کلمـه عبـور سـاده متنـی، شناسـه کاربـری، مـکان و در برخـی مـوارد، سـوابق مالی مانند معاملات بانکی و معاملات مربوط به ارز دیجیتال را افشا می‌کنند.


سـرویس Firebase گـوگل یکـی از محبوب‌ترین پلتفرم‌های توسـعه back-end برای اپلیکیشـن‌های موبایل و وب اسـت کـه یـک پایـگاه داده مبتنـی بـر ابـر را در اختیـار توسـعه‌دهندگان قـرار می‌دهـد، بـه طـوری کـه داده‌هـا را در فرمـت JSON ذخیره نموده و به صورت بلادرنگ با تمام clientهای متصل شده به آن همگام‌سازی می‌کند.

محققـان شـرکت امنیـت موبایـل Appthority، پـی برده‌انـد کـه بسـیاری از توسـعه‌دهندگان اپلیکیشـن نتوانسـته‌اند به درسـتی Firebase خـود را بـا فایـروال هـا و مکانیزم‌هـای احـراز هویت امـن کنند و صدهـا گیگابایت اطلاعات حسـاس از مشتریان خود را در دسترس عموم قرار داده‌اند.

از آنجـا کـه Firebase، همانطـور کـه در زیر نشـان داده شـده اسـت، یـک سـرور API برای دسترسـی به پایـگاه داده‌های میزبانـی شـده توسـط سـرویس، در اختیـار توسـعه‌دهندگان اپلیکیشـن قـرار می‌دهـد، مهاجمـان می‌تواننـد بـا اضافـه کـردن "/.json" بـا یـک نـام پایـگاه داده خالـی در انتهـای نـام میزبـان، بـه داده‌هـای محافظـت نشـده دسترسـی داشته باشند.

Sample API URL: https://<Firebase project name>.firebaseio.com/<database.json>
Payload to Access: Data https://<Firebase project name>.firebaseio.com/.json

محققـان بیـش از ۲/۷ میلیـون برنامـه را اسـکن نمـوده و دریافتنـد کـه بیـش از ۳۰۰۰ برنامـه - ۲۴۴۶ برنامـه‌ی اندرویـدی و ۶۰۰ برنامه‌ی ios- ۲۳۰۰ پایگاه داده با بیش از ۱۰۰ میلیون رکورد را فاش کرده‌اند که در حدود ۱۱۳ گیگابایت داده است.

برنامه‌های آسیب‌پذیر آندروید به تنهایی بیش از ۶۲۰ میلیون بار دانلود شدند.

برنامه‌هـای آسـیب دیـده متعلـق بـه چندیـن دسـته از جملـه مخابـرات، ارز دیجیتـال، مالـی، خدمـات پسـتی، مؤسسات آموزشی، هتل‌ها، بهره‌وری، بهداشت، تناسب اندام، ابزارها و موارد دیگر هستند.

محققـان همچنیـن تجزیـه و تحلیـل مختصـری از داده‌هـای بـه دسـت آمـده از برنامه‌هـای آسـیب‌پذیر را ارائـه نمـوده اند که به شرح ذیل می‌باشد:

- ۲/٦ میلیون کلمه عبور متن ساده و شناسه کاربری
- بیش از ٤ میلیون رکورد داده‌های حفاظت شده‌ی مربوط به سلامت (PHI) (پیام های چت و جزئیات نسخه)
- ۲۵ میلیون رکورد از مکان GPS

| Description | Count | Total % | Android | iOS | Android % | iOS % |
|---|---|---|---|---|---|---|
| Total Apps with FirebaseIO DBs | 28,502 | | 27,227 | 1,275 | 95.53% | 4.47% |
| Apps Vulnerable | 3,046 | 10.69% | 2,446 | 600 | 80.30% | 19.70% |
| % Vulnerable by OS | | | 8.98% | 47.06% | | |
| Total FirebaseIO DB hosts by OS | 21,972 | | 21,193 | 945 | 96.45% | 4.30% |
| FirebaseIO DBs Vulnerable | 2,271 | 10.34% | 1,881 | 440 | 82.83% | 19.37% |
| % Vulnerable by OS | | | 8.88% | 46.56% | | |

- ۵۰،۰۰۰ رکورد از سوابق مالی شامل بانکداری، پرداخت و معاملات Bitcoin
- بیش از ٤/۵ میلیون کلمه رمز (token) از فیسبوک، لینکدین، فایربیس.

محققیـن ادعـا می‌کننـد کـه همـه اینهـا در همـان وهلـه اول اتفـاق می‌افتنـد زیـرا سـرویس Google Firebase به طور پیش‌فـرض داده‌هـای کاربـر را امـن نمی‌کنـد و نیازمنـد آن اسـت کـه توسـعه‌دهندگان بـه طـور صریـح احـراز هویـت کاربـر را در تمـام ردیف‌هـا و جـداول پایـگاه داده پیاده‌سـازی کننـد تـا از پایـگاه داده‌هـای خـود در برابـر دسترسـی غیـر مجاز محافظت کنند.

محققان اظهار داشتند: "تنها ویژگی امنیتی که در دسترس توسعه دهندگان است، احراز هویت (authentication) و مجوز مبتنـی بـر قانـون (rule-based authorization) اسـت." چـه چیـزی بدتـر از ایـن کـه "هیـچ ابـزار ثالثـی جهـت ارائـه رمزگذاری برای آن وجود ندارد!"

پیـش از ایـن، محققـان بـا گـوگل ارتبـاط برقـرار نمـوده و لیسـتی از پایـگاه داده‌هـای آسـیب‌پذیر اپلیکیشـن‌ها را ارائـه داده بودنـد و بـا چنـد توسـعه‌دهنده‌ی اپلیکیشـن نیـز تمـاس گرفتـه و جهـت رفـع مشـکل بـه آن‌هـا کمـک کـرده بودند.

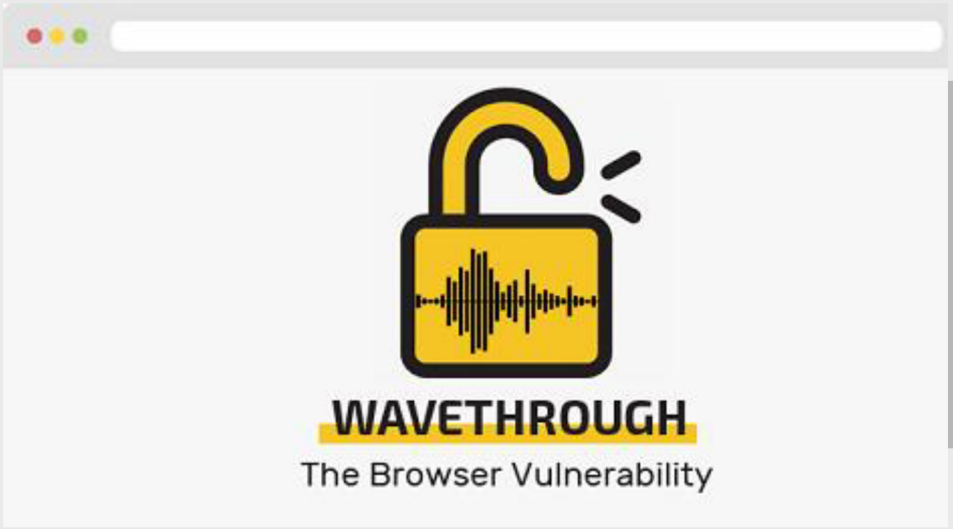
منبع خبر: https://thehackernews.com/۲۰۱۸/۰٦/mobile-security-firebase-hosting.html

# آسیب پذیری

# ۱. کشف باگ حیاتی در مرورگرهای مدرن

آسیب پذیری (گردآورنده: آتوسا خدامرادی)

محققان گوگل آسیب‌پذیری حیاتی جدیدی در مرورگرهای وب کشف نموده‌اند، که به موجب آن مرورگر وب می‌تواند به وب سایتی که شما از آن بازدید کرده‌اید اجازه دهد اطلاعات حساب کاربری که در وب سایت دیگری بر روی همان مرورگر وارد نموده‌اید را سرقت نماید.




این آسیب‌پذیری که توسط یکی از توسعه‌دهندگان گوگل به نام "Jake Archibald" کشف شده است، در مرورگرهایی که درخواست‌های cross-origin را برای ویدیو و صوت پشتیبانی می‌کنند، وجود دارد. به موجب این آسیب‌پذیری هکر می‌تواند با دسترسی از راه دور، محتوای gmail یا پیام‌های خصوصی facebook شما را بخواند.

بنا به دلایل امنیتی، مرورگرهای جدید به وب سایت‌ها اجازه ایجاد درخواست‌های cross-origin را در دامنه‌های مختلف نمی‌دهند مگر اینکه به دامنه‌ای صراحتاً اجازه داده شده باشد. این باعث می‌شود تنها داده‌هایی درخواست شود که از یک سایت یکسان بارگذاری شده باشد، و جلوی درخواست‌هایی از سایت‌های دیگر که سعی در سرقت اطلاعات شما دارند گرفته شود.

Archibald دریافت که مرورگرهای فایرفاکس و Microsoft edge اجازه می‌دهند که عناصر رسانه‌ای برای تلفیق داده های قابل رؤیت و مبهم، یا تلفیق داده‌های مبهمی که از منابع مختلف هستند، یک حمله مصنوعی ایجاد کنند و راه را برای هکرها باز کنند.

این باگ زمانی شروع به کار می‌کند که مرورگرها مجموعه‌ای از درخواست‌ها را برای عناصر رسانه‌ای اجرا می‌کنند.

این حفره امنیتی می‌تواند توسط وب‌سایت‌های مخربی که از فایل‌های رسانه‌ای تعبیه شده در صفحه وب خود بهره می‌برند، مورد استفاده قرار گیرد. به این صورت که هنگام پخش رسانه، فقط محتوای جزئی را از سرور خود ارائه دهند و از مرورگر بخواهند که باقی فایل را از منابع دیگری دریافت کند. به این ترتیب مرورگر را وادار به ایجاد یک درخواست cross-origin می‌کنند.

مرورگرهای سافاری و کروم با استفاده از سیاست‌های امنیتی که از قبل ایجاد کرده‌اند، درخواست‌های cross-origin را محدود کرده و کاربران خود را از این آسیب‌پذیری حفاظت نموده‌اند.

کاربـران این دو مرورگر باید از نصب بودن آخرین نسـخه این مرورگرهـا اطمینان حاصل نمایند.

منبع خبر: https://thehackernews.com/۲۰۱۸/۰٦/browser-cross-origin-vulnerability.html

## ۲. کشف آسیب‌پذیری حیاتی در سیستم کنترل دسترسی سیسکو

آسیب پذیری (گردآورنده: پویان مسعودی‌نیا)

کشـف اسـیب پذیـری حیاتـی در یکـی از دسـتگاه‌های مدیریـت دسترسـی سیسـکو ایـن امـکان را بـه هکرهـا می‌دهد که از راه دور به شـبکه شـرکت‌های بزرگ دسترسی پیدا کنند.


ایـن اختـلال در سیسـتم کنتـرل دسترسـی امن سیسـکو (ACS) یافت شـد که مدیران سیسـتم از آن بـرای تأیید هویـت کاربـران در یـک شـبکه اسـتفاده می‌کننـد، ضمنـاً لازم بـه ذکـر اسـت کـه ایـن آسـیب پذیـری از لحـاظ شـدت حیاتی بودن، نمره ۹/۸ از ۱۰ را کسـب نموده است.

بـه گفتـه دو محقـق امنیتـی کـه ایـن بـاگ را بـه سیسـکو گـزارش داده‌انـد، هکرهـا می‌تواننـد دسترسـی مسـتقیم و سـریع بـه شـبکه داشـته باشـند و اطلاعـات کاربـران و دسترسـی آن‌هـا را تغییـر دهنـد و همچنیـن بـه صـورت "man in the middle" (وجـود یـک سیسـتم در میـان ارتبـاط بـرای سـرقت اطلاعات ) عمل کنند.

"Mikhail Klyuchnikov" کـه ایـن بـاگ را شناسـایی کـرده می‌گویـد: "اگـر سیسـکو (ACS) بـا اکتیـو دایرکتوری مایکروسـافت هماهنـگ باشـد_که اغلـب هـم همینطـور اسـت_ هکـر می‌توانـد اطلاعـات محرمانـه ادمیـن را سـرقت نمایـد. حتـی بـدون یکپارچگـی اکتیـو دایرکتـوری، بـاز هـم هکـر می‌توانـد کنتـرل روترهـا و فایروال‌هـای متصـل شـده را بـرای هدایـت و تغییـر ترافیـک در شـبکه بـه دسـت بگیـرد یـا حتـی بـه نقـاط حسـاس شبکه دسترسی پیدا کند.

مسئله قابل توجه این است که سرور چگونه پیام‌های خود را در AMF۳ هدایت می‌کند، (AMF۳) یک فرمت دودویی است که در زبان‌های برنامه‌نویسی مختلف، از جمله پایتون، پرل، فلش و جاوا مورد استفاده قرار می‌گیرد. در این حالت، مهاجم می‌تواند یک شیء مخرب جاوا را به یک فرمت مناسب برای شبکه‌های مختلف بفرستد، با این کار، زمانی که سرور بارگذاری شود کد مخرب اجرا می‌گردد.

غول شبکه (سیسکو) این باگ را در ماه گذشته برطرف نموده است، این در حالی است که سیستم کنترل دسترسی امن سیسکو تقریباً از سال گذشته به پایان عمر خود رسیده و دیگر به فروش نمی‌رسد!

سخنگوی سیسکو اذعان داشت که مشخص نیست چه تعداد دستگاه تحت تاثیر این آسیب‌پذیری قرار می‌گیرند، و تیم پاسخگویی امنیت محصولات شرکت نیز اظهار داشتند که "تاکنون هیچ گونه خبری مبنی بر استفاده مخرب از این آسیب‌پذیری دریافت نکرده‌اند."

منبع خبر:

https://www.zdnet.com/article/cisco-fixes-critical-bug-that-exposed-networks-to-/hackers

## ۳. ده‌ها آسیب‌پذیری مهم و حیاتی در طیف وسیعی از محصولات سیسکو

آسیب پذیری (گردآورنده: آتوسا خدامرادی)

## ۱.۳ اجرای کد دلخواه NX-API، در سیستم‌عامل NX-OS سیسکو با شناسه CVE-۲۰۱۸-۰۳۰۱

### شدت آسیب‌پذیری

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

### خلاصه آسیب‌پذیری

یک آسیب‌پذیری در قابلیت NX-API از سیستم‌عامل NX-OS سیسکو می‌باشد، که بدون احراز هویت به هکر اجازه می‌دهد که از راه دور بسته‌ای در سیستم آسیب دیده برای مدیریت رابط (interface) ایجاد کند، و به موجب این عمل، سر ریز بافر اتفاق می‌افتد. این آسیب‌پذیری ناشی از اعتبارسنجی نادرست در ماژول احراز هویت زیر سیستم NX-API است. در صورت فعال بودن ویژگی NX-API، هکر می‌تواند از طریق ارسال بسته HTTP یا HTTPS به سیستم آسیب دیده، این آسیب پذیری را اکسپلویت کند و مدیریت رابط سیستم آسیب دیده را به دست گیرد، که البته این ماژول به صورت پیش‌فرض غیر فعال است.

محصولاتی از سیسکو که به موجب اجرای سیستم‌عامل NX-OS این آسیب‌پذیری را دارند شامل موارد زیر هستند:

- سوییچ‌های لایه سه، سری MDS ۹۰۰۰
- محصولات توسعه دهنده، سری Nexus ۲۰۰۰
- سوییچ‌های سری Nexus ۳۰۰۰
- پلتفرم سوییچ‌های Nexus ۳۵۰۰
- پلتفرم سوییچ‌های Nexus ۵۵۰۰
- پلتفرم سوییچ‌های Nexus ۵۶۰۰
- پلتفرم سوییچ‌های Nexus ۶۰۰۰
- سوییچ‌های سری Nexus ۷۰۰۰
- سوییچ‌های سری Nexus ۷۷۰۰
- سوییچ‌های سری Nexus ۹۰۰۰ در حالت NX-OS مستقل
- ماژول‌های فابریک و کارت‌های خطی سری-R از Nexus ۹۵۰۰

### راهکارهای امنیتی ارائه شده تا کنون

تا کنون راهکارهایی برای رفع این آسیب‌پذیری از طرف سیسکو ارائه نشده است، اما بروزرسانی جدیدی از سیسکو منتشر شده است که به این آسیب‌پذیری نیز اشاره دارد. برای کسب اطلاعات بیشتر درباره این بروزرسانی به آدرس زیر مراجعه شود:

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-۲۰۱۸۰۶۲۰-nxos-bo

## ۲.۳ اجرای کد دلخواه در سرویس‌های فابریک سیسکو مربوط به سیستم‌عامل‌های NX-OS و FXOS شرکت سیسکو_ با شناسه CVE-۲۰۱۸-۰۳۰٤

### شدت آسیب‌پذیری

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

### خلاصه آسیب‌پذیری

یک آسیب‌پذیری در مولفه سرویس‌های فابریک سیسکو (CFS)، موجود در سیستم‌عاملهایFXOS وNX-OS شرکت سیسکو می‌باشد. این آسیب‌پذیری، بدون احراز هویت به هکر اجازه می‌دهد که از راه دور، محتوای حافظه حساس را بخواند، وضعیت انکار سرویس ایجاد کند، یا کدهای دلخواه را با دسترسی root اجرا کند. دلیل وجود این آسیب‌پذیری، اعتبارسنجی ناکافی سرآیند بسته‌های سرویس فابریک سیسکو می‌باشد. هکر این آسیب‌پذیری را با ارسال یک بسته سرویس فابریک سیسکو، به سیستم قربانی اکسپلویت می‌کند. اکسپلویت موفق این آسیب‌پذیری باعث سرریز بافر، یا وضعیت overread بافر در مولفه سرویس‌های فابریک سیسکو می‌شود و می‌تواند به هکر اجازه دهد که محتوای حافظه حساس را بخواند، وضعیت انکار سرویس ایجاد کند، یا کدهای دلخواه را با دسترسی root اجرا کند.

محصولاتی از سیسکو که به موجب اجرای سیستم‌عامل‌های FXOS و NX-OS و پیکربندی سرویس‌های فابریک سیسکو، این آسیب‌پذیری را دارند شامل موارد زیر هستند:

- فایروال‌های Next-Generation سری Firepower ٤١٠٠
- دستگاه‌های امنیتی Firepower ۹۳۰۰
- سوییچ‌های لایه سه سری MDS ۹۰۰۰

- توسعه دهنده‌های فابریک سری Nexus ۲۰۰۰
- سوییچ‌های سری Nexus ۳۰۰۰
- پلتفرم سوییچ‌های Nexus ۳۵۰۰
- پلتفرم سوییچ‌های Nexus ۵۵۰۰
- سوییچ‌های سری Nexus ۵۶۰۰
- سوییچ‌های سری Nexus ۶۰۰۰
- سوییچ‌های سری Nexus ۷۰۰۰
- سوییچ‌های سری Nexus ۷۷۰۰
- سوییچ‌های سری Nexus ۹۰۰۰ در حالت NX-OS مستقل
- ماژول‌های فابریک و کارت‌های خطی سری-R از Nexus ۹۵۰۰
- اتصالات فابریک سری UCS ۶۱۰۰
- اتصالات فابریک سری UCS ۶۲۰۰
- اتصالات فابریک سری UCS ۶۳۰۰

### راهکارهای امنیتی ارائه شده تا کنون

تا کنون راهکارهایی برای رفع این آسیب‌پذیری از طرف سیسکو ارائه نشده است، اما بروزرسانی جدیدی از سیسکو منتشر شده است که به این آسیب‌پذیری نیز اشاره دارد. برای کسب اطلاعات بیشتر درباره این بروزرسانی به آدرس زیر مراجعه شود:

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

**منبع خبر:**

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۰۶۲۰-fxnxos-ace

## ۳.۳ اجرای کد دلخواه در سرویس‌های فابریک سیسکو مربوط به سیستم‌عامل‌های NX-OS و FXOS شرکت سیسکو_ با شناسه CVE-۲۰۱۸-۰۳۰۸

### شدت آسیب‌پذیری

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

## خلاصه آسیب‌پذیری

یک آسیب‌پذیری در مولفه سرویس‌های فابریک سیسکو (CFS)، موجود در سیستم‌عاملهای FXOS و NX-OS شرکت سیسکو می‌باشد. این آسیب‌پذیری ناشی از اعتبارسنجی نا کافی مقادیر سرآیند بسته‌های سرویس فابریک سیسکو می‌باشد. هکر این آسیب‌پذیری را با ارسال یک بسته سرویس فابریک سیسکو، به سیستم قربانی اکسپلویت می‌کند. اکسپلویت موفق این آسیب‌پذیری، باعث سرریز بافر در سیستم قربانی می‌شود و می‌تواند باعث بروز وضعیت انکار سرویس شود.

محصولاتی از سیسکو که به موجب اجرای سیستم‌عامل‌های FXOS و NX-OS و پیکربندی سرویس‌های فابریک سیسکو، این آسیب‌پذیری را دارند شامل موارد زیر هستند:

- فایروال‌های Next-Generation سری Firepower ۴۱۰۰
- دستگاه‌های امنیتی Firepower ۹۳۰۰
- سوییچ‌های لایه سه سری MDS ۹۰۰۰
- توسعه دهنده‌های فابریک سری Nexus ۲۰۰۰
- سوییچ‌های سری Nexus ۳۰۰۰
- پلتفرم سوییچ‌های Nexus ۳۵۰۰
- پلتفرم سوییچ‌های Nexus ۵۵۰۰
- سوییچ‌های سری Nexus ۵۶۰۰
- سوییچ‌های سری Nexus ۶۰۰۰
- سوییچ‌های سری Nexus ۷۰۰۰
- سوییچ‌های سری Nexus ۷۷۰۰
- سوییچ‌های سری Nexus ۹۰۰۰ در حالت NX-OS مستقل
- ماژول‌های فابریک و کارت‌های خطی سری-R از Nexus ۹۵۰۰
- اتصالات فابریک سری UCS ۶۱۰۰
- اتصالات فابریک سری UCS ۶۲۰۰
- اتصالات فابریک سری UCS ۶۳۰۰

## راهکارهای امنیتی ارائه شده تا کنون

تا کنون راهکارهایی برای رفع این آسیب‌پذیری از طرف سیسکو ارائه نشده است، اما بروزرسانی جدیدی از سیسکو منتشر شده است که به این آسیب‌پذیری نیز اشاره دارد. برای کسب اطلاعات بیشتر درباره این بروزرسانی به آدرس زیر مراجعه شود:

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-۲۰۱۸۰۶۲۰-fxnxos-fab-ace

## ٤.٣ آسیب‌پذیری اجرای کد خودسرانه در سرویس های فابریک سیسکو مربوط به سیستم عامل های NX-os و_ FX-os با شناسه CVE-۲۰۱۸-۰۳۱٤

### شدت آسیب‌پذیری

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

### خلاصه آسیب‌پذیری

وجود یک اسیب پذیدی در مؤلفه سرویس‌های فابریک سیسکو (CFS) مربوط به سیستم عامل‌های FX-os و NX-os شرکت سیسکو که این اجازه را به هکر می‌دهد تا بدون احراز هویت از راه دور موفق به اجرای کد خودسرانه شود .

دلیل این اسیب پذیری این است که در زمان پردازش داده های بسته نرم افزار اعتبار سنجی کافی در هدر های بسته سرویس های فابریک سیسکو صورت نمیگیرد.

هکر می‌تواند این آسیب‌پذیری را با ارسال یک بسته مخرب سرویس فابریک سیسکو (CFS) ، به سیستم قربانی اکسپلویت کند. اکسپلویت موفق این آسیب‌پذیری، باعث ایجاد وضعیت سرریز بافر در سیستم قربانی می‌شود که هکر قادر به اجرای کد خودسرانه خود می‌شود.

محصولاتی از سیسکو که به موجب اجرای سیستم عامل FXOS و NX-OS و پیکربندی سرویس‌های فابریک سیسکو، این آسیب‌پذیری را دارند شامل موارد زیر هستند:

- فایروال‌های Next-Generation سری Firepower ٤١٠٠
- دستگاه‌های امنیتی Firepower ٩٣٠٠
- سوییچ‌های لایه سه سری MDS ٩٠٠٠
- توسعه دهنده‌های فابریک سری Nexus ٢٠٠٠
- سوییچ‌های سری Nexus ٣٠٠٠
- پلتفرم سوییچ‌های Nexus ٣٥٠٠
- پلتفرم سوییچ‌های Nexus ٥٥٠٠
- سوییچ‌های سری Nexus ٥٦٠٠
- سوییچ‌های سری Nexus ٦٠٠٠
- سوییچ‌های سری Nexus ٧٠٠٠

- سوییچ‌های سری Nexus ۷۷۰۰
- سـوییچ‌های سری Nexus ۹۰۰۰ در حالت NX-OS مستقل
- ماژول‌های فابریک و کارت‌های خطی سـری-R از Nexus ۹۵۰۰
- اتصالات فابریک سری UCS ۶۱۰۰
- اتصالات فابریک سری UCS ۶۲۰۰
- اتصالات فابریک سری UCS ۶۳۰۰

راهکارهای امنیتی ارائه شـده تا کنون

راهکارهایـی بـرای رفـع ایـن آسـیب‌پذیری از طـرف شـرکت سیسـکو ارائـه نشـده اسـت، امـا بروزرسـانی جدیـدی از سیسـکو منتشـر شـده اسـت کـه بـه ایـن آسـیب‌پذیری نیـز اشـاره دارد. بـرای کسـب اطلاعـات بیشـتر درباره این بروزرسانی به آدرس زیر مراجعه شود:

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-۲۰۱۸۰۶۲۰-fx-os-fabric-execution

## ۵.۳ آسـیب‌پذیری اجـرای کـد خودسـرانه در سـرویس هـای فابریـک سیسـکو مربـوط بـه سیسـتم عامـل هـای NX-os و FX-os _با شناسه CVE-۲۰۱۸-۰۳۱۲

### شدت آسیب‌پذیری

با توجه به گزارشـات منتشـر شده، شدت این آسیب پذیری Critical می‌باشد.

### خلاصه آسیب‌پذیری

وجود یک اسـیب پذیدی در مؤلفه سـرویس های فابریک سیسـکو (CFS) مربوط به سیسـتم عامل های FX-os و NX-os شـرکت سیسـکو کـه ایـن اجـازه را بـه هکـر مـی دهـد تـا بـدون احـراز هویـت از راه دور موفـق بـه اجرای کد خودسـرانه شـود و همچنین سـبب ایجاد وضعیت (DOS) روی دستگاه آسیب پذیر شود.

دلیـل ایـن اسـیب پذیـری ایـن اسـت کـه در زمـان پـردازش داده هـای بسـته نـرم افـزار اعتبـار سـنجی کافـی در هدر های بسـته سـرویس های فابریک سیسکو صورت نمی گیرد.

هکـر مـی توانـد ایـن آسـیب‌پذیری را با ارسـال یک بسـته مخـرب سـرویس فابریک سیسـکو (CFS) ، به سیسـتم قربانـی اکسـپلویت کند. اکسـپلویت موفـق این آسـیب‌پذیری، باعث ایجاد وضعیت سـرریز بافـر همچنین وضعیت (DOS) در سیسـتم قربانی می‌شـود که هکر قادر به اجرای کد خودسـرانه خود می شود.

محصولاتی از سیسکو که به موجب اجرای سیستم عامل FXOS و NX-OS و پیکربندی سرویس‌های فابریک سیسکو، این آسیب‌پذیری را دارند شامل موارد زیر هستند:

- فایروال‌های Next-Generation سری Firepower ۴۱۰۰
- دستگاه‌های امنیتی Firepower ۹۳۰۰
- سوییچ‌های لایه سه سری MDS ۹۰۰۰
- توسعه دهنده‌های فابریک سری Nexus ۲۰۰۰
- سوییچ‌های سری Nexus ۳۰۰۰
- پلتفرم سوییچ‌های Nexus ۳۵۰۰
- پلتفرم سوییچ‌های Nexus ۵۵۰۰
- سوییچ‌های سری Nexus ۵۶۰۰
- سوییچ‌های سری Nexus ۶۰۰۰
- سوییچ‌های سری Nexus ۷۰۰۰
- سوییچ‌های سری Nexus ۷۷۰۰
- سوییچ‌های سری Nexus ۹۰۰۰ در حالت NX-OS مستقل
- ماژول‌های فابریک و کارت‌های خطی سری-R از Nexus ۹۵۰۰
- اتصالات فابریک سری UCS ۶۱۰۰
- اتصالات فابریک سری UCS ۶۲۰۰
- اتصالات فابریک سری UCS ۶۳۰۰

## راهکارهای امنیتی ارائه شده تا کنون

راهکارهایی برای رفع این آسیب‌پذیری از طرف شرکت سیسکو ارائه نشده است، اما بروزرسانی جدیدی از سیسکو منتشر شده است که به این آسیب‌پذیری نیز اشاره دارد. برای کسب اطلاعات بیشتر درباره این بروزرسانی به آدرس زیر مراجعه شود:

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-۲۰۱۸۰۶۲۰-fx-os-cli-execution

# ۴. آسیب‌پذیری در سرویس‌های امنیتی (AAA) در IOS XE سیسکو

آسیب پذیری (گردآورنده: آرزو حسنی)

شدت آسیب‌پذیری:

Critical

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

خلاصه آسیب‌پذیری

یک آسیب‌پذیری بحرانی با شناسه CVE-۲۰۱۸-۰۳۱۵درسرویس‌های امنیتیauthentication , authorization accounting (AAA) نرم‌افزارIOS XE سیسکوکشف شده است، در این آسیب‌پذیری مهاجم از راه دور می‌تواند بدون احراز هویت برروی دستگاه آسیب‌دیده کدهای دلخواه اجرا کند یا دستگاه آسیب دیده را مجددا reload کند

این آسیب پذیری ناشی از عملیات نادرست حافظه است که نرم افزار تحت تاثیر قرار می‌گیرد. زمانی که نرم افزار یک نام کاربری را در هنگام احراز هویت ورود تحلیل می‌کند. مهاجم می‌تواند با بهره‌گیری از این آسیب‌پذیری، با تلاش برای تأیید اعتبار به یک دستگاه آسیب دیده مورد استفاده قرار دهد. بهره‌برداری موفق می‌تواند به مهاجم اجازه دهد کد دلخواه را بر روی دستگاه آسیب دیده اجرا کند یا موجب شود که دستگاه آسیب دیده مجددا reloadشود و در نتیجه حمله Dos انجام شود.

راهکارهای امنیتی ارائه شده تا کنون.

۱- سیسکو به‌روز رسانی‌های نرم‌افزاری که مربوط به این آسیب پذیری می‌باشد را منتشر نموده است. هیچ راه‌حلی برای این آسیب‌پذیری وجود ندارد. با این حال، مدیران ممکن است دستگاه‌های در معرض خطر را توسط محدود نمودن نشست‌های مدیریتی دستگاه محدود کنند.

با استفاده از دسترسی vty فقط اجازه دسترسی به دستگاه‌های شناخته شده و قابل اعتماد برای اتصال به دستگاه را می‌دهیم، مدیران می‌توانند اطمینان حاصل کنند که تنها توسط منابع قابل اعتماد با استفاده از vty به یک دستگاه دسترسی یابند. مثال زیر یک دسترسی vty را نشان می‌دهد که اجازه دسترسی vty به یک دستگاه از تنها توسط رنج ۱۹۲.۱۶۸.۱.۰/۲۴و آدرس IP ۱۷۲/۱۶/۱/۲ را می‌دهد و دسترسی vty از هر جای دیگر را رد می‌کند:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

۲- در رابطه با پورت‌های کنسول یا پورت‌های کمکی که از طریق یک اتصال به ترمینال سرور متصل می‌شوند اطمینان حاصل شود که دسترسی Vty در ترمینال سرور پیکربندی شده است. برای پورت‌های کنسول یا پورت‌های کمکی که متصل نیستند و یا مورد استفاده قرار نمی‌گیرند، دستور no exec را روی line برای جلوگیری از دسترسی به آن پورت وارد کنید. همانطور که در مثال زیر نشان داده شده است:

```
Router(config)# line aux 0
Router(config-line)# no exec
```

منابع:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۰۶۰۶-aaa

## ۵. آسیب‌پذیری (PCP) ناشی از نامعتبر بودن RMI

آسیب پذیری (گردآورنده: آرزو حسنی)

### شدت آسیب‌پذیری

Critical

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

### خلاصه آسیب‌پذیری

یک آسیب‌پذیری بحرانی در نرم‌افزار Prime Collaboration Provisioning سیسکو کشف شده است. می‌تواند اجازه نامعتبر کردن اعتبار سنجی به مهاجم در دسترسی از راه دور به سیستم Remote Method Invocation ( RMI ) جاوا را صادر کند.

این آسیب‌پذیری ناشی از پورت باز در رابط شبکه و پیکربندی سرویس موتور (NICE) است. مهاجم می‌تواند با دسترسی به سیستم باز RMI روی یک نمونه PCP که تحت تاثیر قرار گرفته است از این آسیب پذیری بهره برداری کند. این‌آسیب‌پذیری به مهاجم اجازه می‌دهد تا اقدامات مخرب بر روی PCP و دستگاه‌هایی که به آن وصل شده‌اند انجام دهد. شناسه این آسیب‌پذیری CVE-۲۰۱۸-۰۳۲۱ است.

### راهکارهای امنیتی ارائه شده تا کنون

سیسکو به‌روز رسانی‌های نرم افزاری را که مربوط به این آسیب پذیری است، منتشر کرده است. هیچ راه حل هایی برای این آسیب پذیری وجود ندارد.

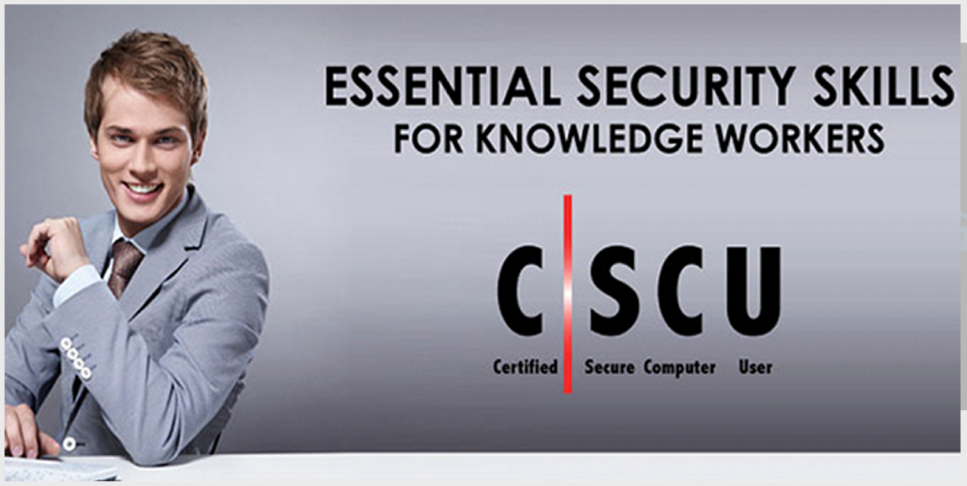
منابع : https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-۲۰۱۸۰۶۰۶-fprime-rmi

# امنیت کاربر رایانه

مرکز تخصصی آپا دانشگاه رازی

# امنیت کاربر رایانه CSCU

هر کاربر رایانه باید روش حفاظت از دارایی‌های اطلاعاتی خود و نحوه اتصال ایمن به سیستم‌های دیگر را در شبکه بداند. دوره آموزشی امنیت کاربر رایانه، دانش امنیت اطلاعات و شبکه یک کاربر رایانه را در استفاده از منابع رایانه‌ای در داخل شبکه سازمان و یا حین اتصال به اینترنت ارتقا می‌دهد. اخذ گواهینامه این دوره، بیانگر آن است که دارنده این مدرک، شایستگی و دانش استفاده از مهارت‌های شبکه‌های رایانه‌ای را دارا بوده و مفاهیم ضروری امنیت اطلاعات را می‌داند.

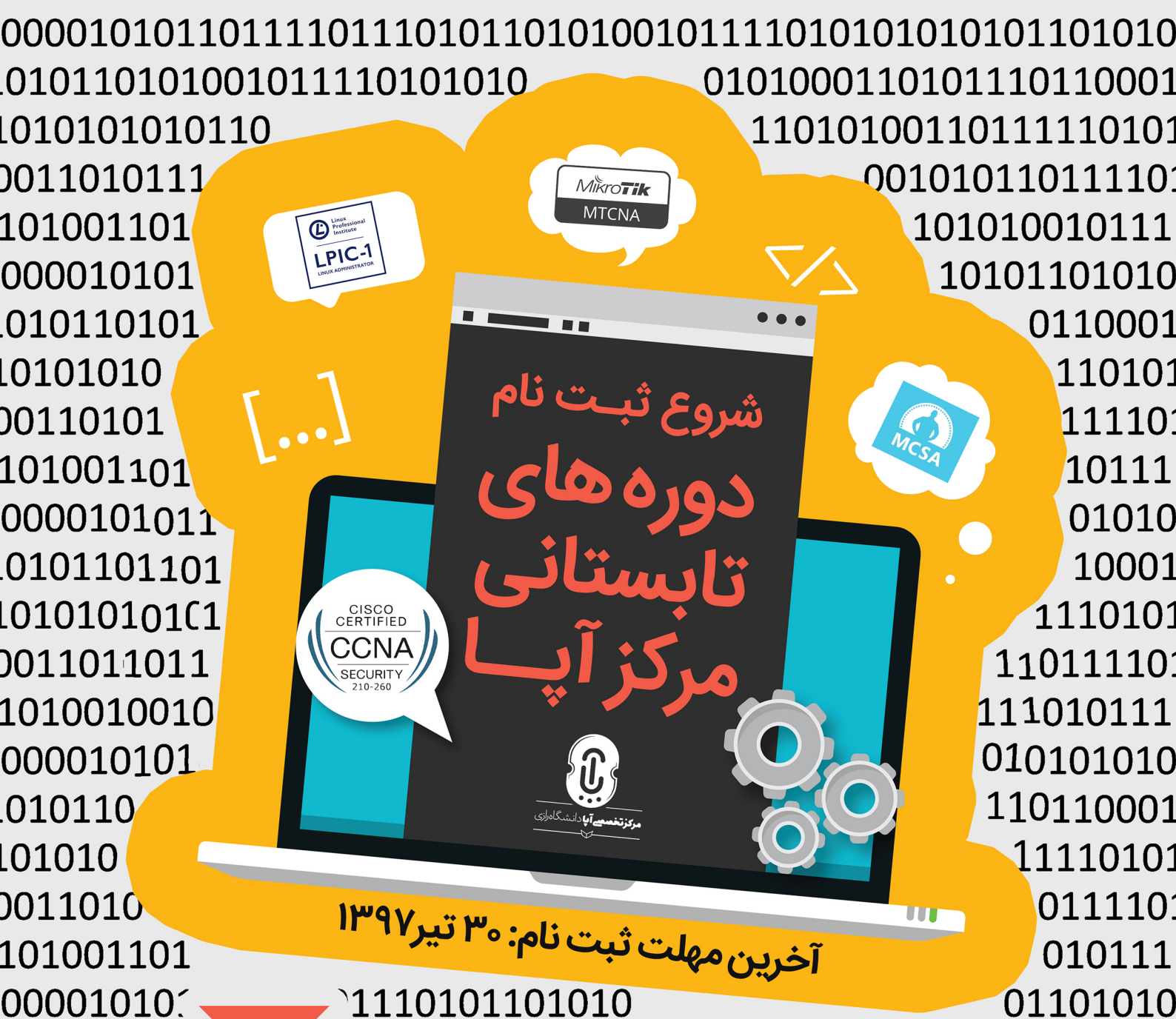



## خبر خوب این است که:

ما در هر شماره از بولتن خبری خود بخشی از مطالب این دوره آموزشی را به صورت رایگان در اختیار شما عزیزان قرار می‌دهیم، با دنبال نمودن این مطالب آموزشی:

- ☑ سطح امنیتی شما، که یک کاربر رایانه شخصی هستید ارتقاء خواهد یافت.
- ☑ توانایی شناسایی تهدیدهای سایبری را خواهید داشت.
- ☑ با روش‌های افزایش امنیت رایانه‌های شخصی در محیط‌های مجازی و شبکه‌های سازمانی آشنا خواهید شد.

## در هفته‌نامه‌های بعدی ما منتظر مطالب آموزشی " امنیت کاربر رایانه " باشید.




| | عنوان فارسی دوره | عنوان انگلیسی دوره | طول دوره | هزینه دوره | نام مدرس |
|---|---|---|---|---|---|
| ۱ | دوره آموزشی امنیت شبکه سیسکو | CCNA Security | ۴۵ ساعت | ۵۵۰/۰۰۰ تومان | مهندس مهدی اسفندیاری |
| ۲ | دوره مدیریت شبکه های مبتنی بر سرور ۲۰۱۶ و رویکرد امن آن | MCSA 2016 | ۶۰ ساعت | ۵۰۰/۰۰۰ تومان | مهندس مهدی اسفندیاری |
| ۳ | دوره آموزشی مقدماتی لینوکس | LPIC-1 | ۵۰ ساعت | ۵۰۰/۰۰۰ تومان | دکتر وحید زنگنه |
| ۴ | دوره آموزشی میکروتیک | MTCNA | ۴۰ ساعت | ۳۵۰/۰۰۰ تومان | مهندس سعید نادری |

جهت ثبت نام و کسب اطلاعات بیشتر با ما تماس بگیرید:

@Edu_Aparazi ۳۴۲۷۳۳۹۰ cert.razi.ac.ir