شماره بیست و پنجم - بهمن ۱۳۹۷

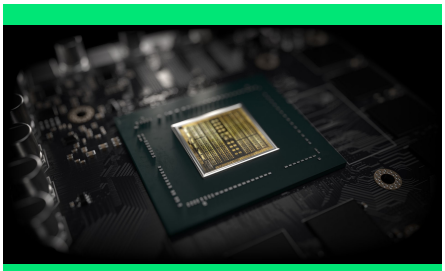
خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

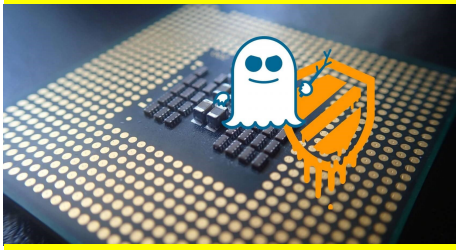
حمله سایبری ایالات متحده به آژانس اینترنتی روسیه

کشمکش‌های بین دو ابر قدرت امریکا و روسیه سال‌هاست که وجود دارد که گاهی اوقات این درگیری‌ها شدت می‌گیرد. با توسعه‌ی فناوری اطلاعات و فضاهای سایبری، این جنگ به این زمینه نیز کشیده است و این دو کشور هر از چندگاهی برای نشان دادن قدرت خود اقدام به انجام حملات سایبری بر علیه یکدیگر می‌کنند. - صفحه ۲



آپدیت جدید Nvidia آسیب پذیری‌های خطرناک آن را رفع می‌کند.

در جدیدترین به روز رسانی درایور Nvidia هشت آسیب پذیری جدی امنیتی در آن پوشش داده و مرتفع گردید. این آسیب پذیری‌ها می‌توانستند منجر به افزایش سطح دسترسی، اجرای کد، افشای اطلاعات شوند. - صفحه ۳

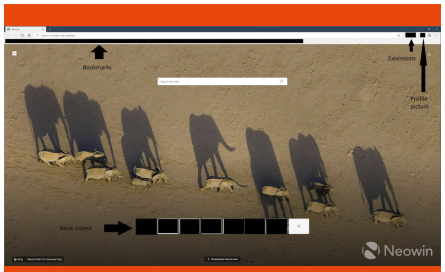


آسیب پذیری Spectre تا یکسال آینده ادامه دارد!

محققان گوگل می‌گویند که وصله‌های نرم افزاری برای آسیب پذیری Spectre نمی‌توانند به طور کامل در برابر این نقص تدابیر محافظتی را اجرا کنند و حداقل تا ۱ سال آینده این آسیب پذیری در کنار ما خواهد ماند. - صفحه ۴

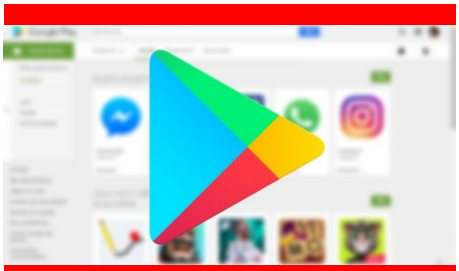
شرکت ICANN به دنبال استقرار برنامه‌های امنیتی سخت‌تر

ICANN سازمانی نیمه دولتی است، که از هدف‌های این شرکت ثبات در عملکرد اینترنت و توسعه سیاست‌های اهداف از پیش تعریف شده، مدیریت و بررسی مسایل فنی DNS در سطح جهانی اینترنت است. - صفحه ۵



اولین اسکرین شات از مرورگر مایکروسافت با موتور کروم!

چندماهی است که از تایید مایکروسافت در خصوص ساخت یک مرورگر با اسم رمز Anaheim بر مبنای کروم می‌گذرد که امروز تصاویری از آن در فضای اینترنت پخش شد. - صفحه ۶



حذف ۱ میلیون اپلیکیشن از Google Play

شرکت گوگل در طول سال‌ها چندین بار اقدام به حذف اپلیکیشن‌هایی کرده است که از نظر آنان کاربران را مورد تهدید قرار داده‌اند. این اپلیکیشن‌ها هرکدام عموما دارای نقص‌های امنیتی می‌باشند که موجب آسیب پذیری کاربران ویا سو استفاده از آنان می‌شود. - صفحه ۷

حمله سایبری ایالات متحده به آژانس اینترنتی روسیه

کشمکش‌های بین دو ابر قدرت امریکا و روسیه سال‌هاست که وجود دارد که گاهی اوقات این درگیری‌ها شدت می‌گیرد. با توسعه‌ی فناوری اطلاعات و فضاهای سایبری، این جنگ به این زمینه نیز کشیده است و این دو کشور هر از چندگاهی برای نشان دادن قدرت خود اقدام به انجام حملات سایبری بر علیه یکدیگر می‌کنند.

در یک نمایش آنلاین، فرماندهی سایبری آمریکا در روزهای انتخابات میان دوره‌ای ۲۰۱۸ توانست به آژانس تحقیقاتی بین المللی روسیه (IRA) دسترسی پیدا کند. به نظر می رسد که این حمله بیشتر حاوی یک پیام باشد تا آسیب رساندن به IRA.

افراد آگاه با این مشکل به Washington Post گفتند که "آنان توانستند IRA را آفلاین کنند." برای یک روز یا بیشتر. این کار برای جلوگیری از روسیه در پخش اطلاعات نادرست در هنگام انجام فرآیند رای گیری اتفاق افتاده است.

IRA به خاطر نقشش در تأثیرگذاری بر کمپین ریاست جمهوری سال ۲۰۱۶ و کاستن اختلاف در رسانه های اجتماعی شناخته شده است. مأموران فدرال ایالات متحده بر این باورند که IRA توسط Yevgeniy Prigozhin، یک oligarch روسیه با پیوندهای نزدیک با پوتین، تامین می شود.

قدرت Cybercom توسط رییس جمهور امریکا برای گسترش حملات سایبری افزایش پیدا کرده است و این عمل، اولین اقدام در استراتژی جدید تعیین شده بود. در زمان شروع این استراتژی، حملات عموم نبودند اما حال با گذشت زمان حملات سیر عمومی پیدا کرده اند.

این اولین باری نیست که IRA هدف حملات ایالات متحده قرار میگیرد. چندین ماه پیش، اعضای Cybercom در پیامی مستقیم، IRA را از دسترس خارج نمودند تا نتوانند برروی انتخابات تاثیر گذار باشند.

مقامات امریکایی مطمئن نیستند که حمله اخیر در طولانی مدت چه تاثیری خواهد گذاشت، اما امیدوارند که این امر نشان دهده ی تصمیم جدی ایالات متحده در خصوص جلوگیری از دخالت های بیشتر روسیه شود.

گردآورنده: محمد مرتضوی

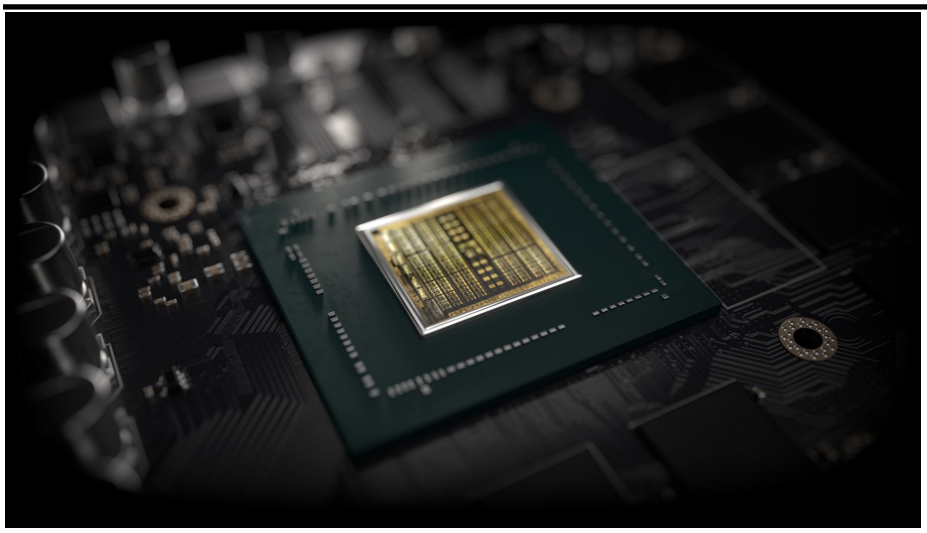
آپدیت جدید Nvidia آسیب پذیری‌های خطرناک آن را رفع می‌کند.

در جدیدترین به روز رسانی درایور Nvidia هشت آسیب پذیری جدی امنیتی در آن پوشش داده و مرتفع گردید. این آسیب پذیری‌ها می‌توانستند منجر به افزایش سطح دسترسی، اجرای کد، افشای اطلاعات شوند. از آنجا که این آسیب پذیری‌ها نیاز به دسترسی مستقیم به دیوایس مربوطه داشتند، لذا در فضای شبکه‌ای امکان دسترسی به این آسیب پذیری‌ها وجود نداشت.

حملات DoS می‌تواند یک کامپیوتر و یا پردازنده گرافیکی را غیرقابل استفاده کند، یا به وسیله یک سو استفاده از آن، می‌تواند آن را اداره کند.

افزایش سطح دسترسی می‌تواند به دو صورت عمل، یکی اینکه مهاجم می‌تواند به سایر کاربران امکان دسترسی به اطلاعات را بدهد. با اینکه می‌تواند امکان کنترل کامپیوتر را در اختیار آنان قرار دهد.

به هر کدام از این هشت آسیب پذیری یک شناسه تعلق گرفته است که عبارتند از CVE-2019-5665 تا CVE-2019-5671.



این آسیب پذیری‌ها در رتبه بندی سیستم CVSS دارای رنج گسترده‌ای هستند و تقریبا از کمترین شدت تا بیشترین آن را پوشش می‌دهند.

آسیب پذیری که در این جدول دارای امتیاز ۸.۸ می‌باشد نیاز به دسترسی محلی دارد. همچنین آسیب پذیری‌هایی با امتیاز کمتر نیاز به دسترسی‌های کمتری دارند.

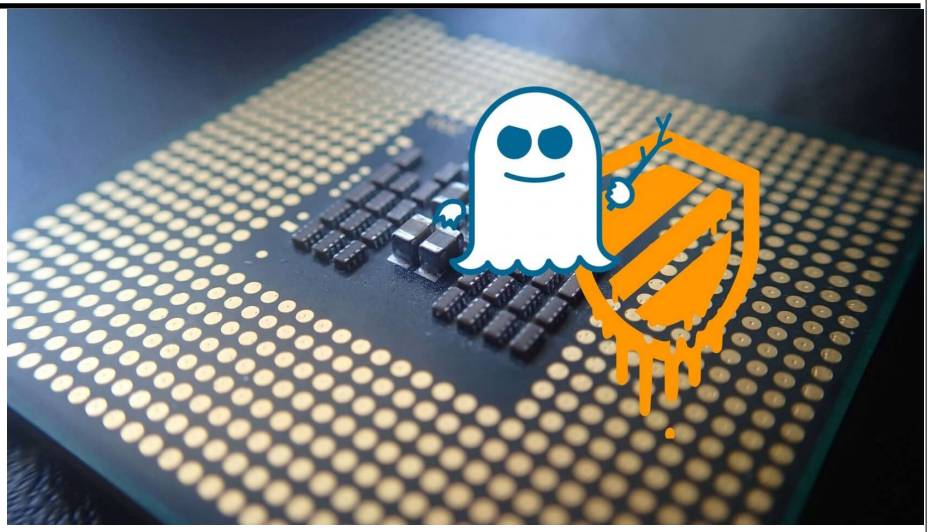
اگر چه در فضای اینترنت هیچ بدافزاری برای سو استفاده از اسن آسیب پذیری‌ها یافت نمی‌شود اما توصیه می‌شود تا کاربران درایورهای خود را در اسرع وقت به جدیدترین به روزرسانی موجود ارتقاع دهند.

برای به روز رسانی درایور خود به برنامه GeForce Experience مراجعه کرده و از بخش Drivers دکمه Check for Updates را انتخاب کنید.

	5665	5666	5667	5668	5669	5670	5671	6260
Denial of Service	✓	✓	✓	✓	✓	✓	✓	
Privilege Escalation	✓	✓	✓	✓	✓	✓		
Code Execution	✓		✓			✓		
Information Disclosure						✓		✓
CVSS Score	8.8	8.8	8.8	8.8	8.8	7.8	6.5	2.2

گردآورنده: محمد مرتضوی

آسیب پذیری Spectre تا یکسال آینده ادامه دارد!



محققان گوگل می‌گویند که وصله‌های نرم افزاری برای آسیب پذیری Spectre نمی‌توانند به طور کامل در برابر این نقص تدابیر محافظتی را اجرا کنند و حداقل تا ۱ سال آینده این آسیب پذیری در کنار ما خواهد ماند.

در واقع، اگر شما در طول سال ۲۰۱۸ فعال در اینترنت باشید، ممکن است به یاد داشته باشید Meltdown و Spectre دو مورد از بزرگترین نقاط ضعف امنیتی سخت افزار است که صنعت فن آوری تا به حال دیده است.

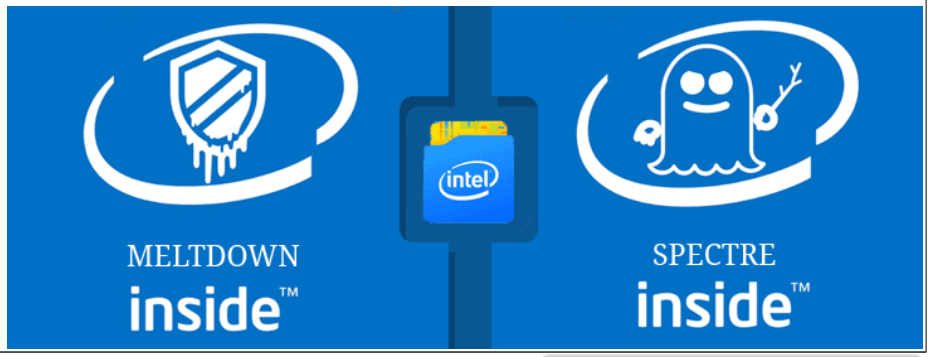
در گذشته جزئیات نقص مورد بحث قرار داده شده است. تقریبا تمام پردازنده‌های مدرن از

در گذشته جزئیات نقص مورد بحث قرار داده شده است. تقریبا تمام پردازنده‌های مدرن از تکنیکی به نام "اعداد احتمالی" برای افزایش کارایی و سرعت محاسباتی استفاده می‌کنند Meltdown و Spectre به لحاظ نظری، مهاجمین را قادر می‌سازد تا اطلاعات شخصی ذخیره شده در مرورگرها، رمز عبور کاربران و سایر قسمت-های معین ماشین را بدون هیچگونه شواهدی پشت سر بگذارند.

وصله‌هایی برای این نقص‌ها تا کنون ارائه شده‌اند اما ایده آل نیستند. در یک مقاله پژوهشی که توسط تیم امنیتی گوگل منتشر شده است توضیح می‌دهد که چرا این موارد نا کارآمد هستند.

محققان امنیتی می‌گویند که اصلاحات مبتنی بر نرم افزار به اندازه کافی برای محافظت از کاربران در برابر تمام مدل‌های Spectre و Meltdown کافی نیست.

محققان حمله Spectre را توسعه دادند تا در این باره اطلاعات بیشتری به دست بیاورند ولی متوجه شدند که هیچ وصله نرم افزاری یا راه حل شناخته شده‌ای در حال حاضر وجود ندارد. شاید باید منتظر چیپ‌های جدید یا سخت افزارهای جدیدی باشیم تا توانایی مقابله با این آسیب پذیری در آنان به صورت Buit In قرار داه شده باشد.



گردآورنده: امیرحسین ضرغامی

شرکت ICANN به دنبال استقرار برنامه‌های امنیتی سخت‌تر

ICANN سازمانی نیمه دولتی است، که از هدف‌های این شرکت ثبات در عملکرد اینترنت و توسعه سیاست‌های اهداف از پیش تعریف شده، مدیریت و بررسی مسایل فنی DNS در سطح جهانی اینترنت است.

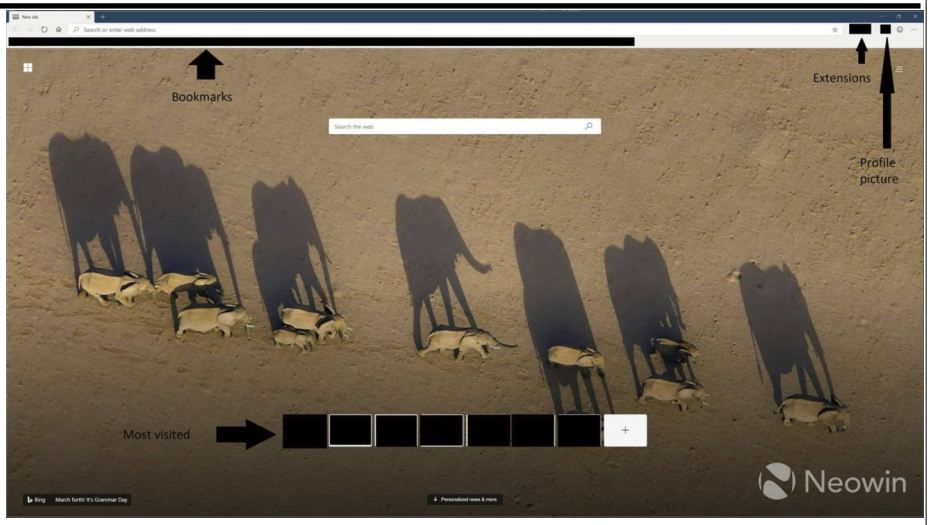
ICANN دفترچه آدرس جهانی است که بر سیستم نام دامنه (DNS) نظارت می‌کند. این سیستم نام دامنه‌ای را که کاربر به مرورگر خود وارد می‌کند، می‌گیرد و آن را به یک آدرس عددی منحصر به فرد تبدیل می‌کند تا افراد را به وب سایت‌هایی که مایل به بازدید آن هستند، مرتبط کند. اما بر اساس اعلام روز جمعه ICANN، زیرساخت DNS توسط افراد خرابکاری هدف قرار گرفته است.

ICANN در پاسخ به حملات DNS، خواستار استقرار کامل سیستم‌های امنیتی نام دامنه یا همان (DNSSEC) می‌باشد. DNSSEC یک تکنولوژی است که اطلاعات را به صورت دیجیتالی "نشانه‌ها" را تأیید می کند تا اعتبار آن را تأیید کند و به این ترتیب مردم از بدرفتاری با وب سایت-هایی که قصد بازدید از آنها را دارند دور بمانند. این یک ابزار موثر در کمک به جلوگیری از حملات "مرد میانی" است که کلاهبرداران می"توانند مردم را به سایت"های مخرب هدایت کنند و آن‌ها را به افشای مدارک ورود، جزئیات پرداخت یا سایر اطلاعات شخصی مجبور کنند.

این آخرین اعلامیه از ICANN کمتر از دو هفته پس از اعلام فهرست چک لیست ثبت دامنه‌ها و فروشندگان برای کمک به تقویت امنیت خود در پی حملات می‌آید. در حالی که ICANN اذعان دارد که راه حل‌های پیشنهادی خود، از جمله اجرای کامل DNSSEC، تمام مشکلات امنیتی اینترنت را حل نخواهد کرد، هر گونه اقداماتی که برای کاهش خطر ضروری است، باید به طور گسترده‌ای انجام شود.

گردآورنده: امیرحسین ضرغامی

اولین اسکرین شات از مرورگر مایکروسافت با موتور کروم!



چندماهی است که از تایید مایکروسافت در خصوص ساخت یک مرورگر با اسم رمز Anaheim بر مبنای کروم می‌گذرد که امروز تصاویری از آن در فضای اینترنت پخش شد.

Neowin با انتشار عکس‌هایی از این مرورگر در حال توسعه نشان داد که این نسخه بسیار شبیه ترکیبی از مرورگر Chrome و Edge می‌باشد. این مرورگر دارای اکثر عناصر محبوب‌ترین مرورگر دینا، یعنی Chrome می‌باشد. همچنین دارای تصویر پروفایل و آیکون مربوط به علاقمندی‌ها می‌باشد.

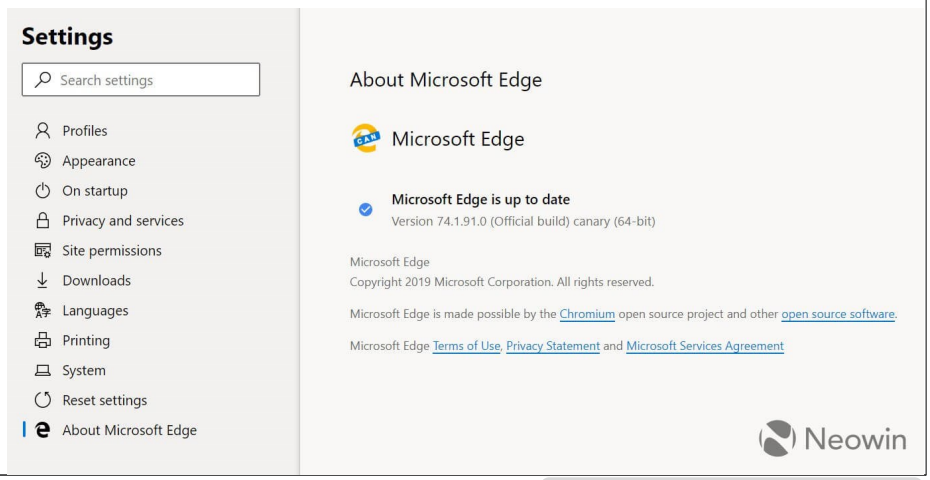
این مرورگر همچنین دارای صفحه‌ی مربوط به افزونه‌های جدید نیز می‌باشد که افراد می‌توانند از این صفحه به افزونه‌های جدید که از فروشگاه Chrome انتقال پیدا کرده‌اند، دسترسی داشته باشند.

از آنجایی که این مرورگر متعلق به مایکروسافت است موتور جستجوی ارائه شده در آن Bing می‌باشد و در پایین صفحه افراد می‌توانند به اخبار Microsoft News دسترسی داشته باشند و بر اساس سلیقه خود آن را شخصی سازی نمایند.

تا این لحظه این مرورگر بسیار شبیه Chrome است اما تا تکمیل شدن نسخه نهایی، تغییرات زیادی در آن به احتمال زیاد رخ خواهد داد.

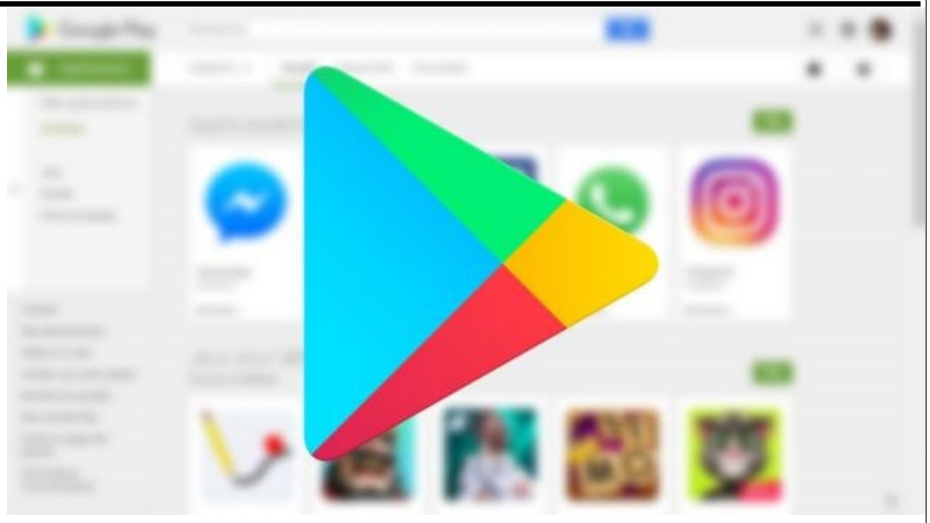
تا زمان انتشار این مرورگر حرف دیگری باقی نمی‌ماند. اما افرادی که مایل هستند تا پیش از همه این مرورگر را دریافت نمایند می‌توانند در لینک زیر ثبت نام نمایند.

microsoftedgeinsider.com/en-us



گردآورنده: امیرحسین ضرغامی

حذف ۱ میلیون اپلیکیشن از Google Play



شرکت گوگل در طول سال‌ها چندین بار اقدام به حذف اپلیکیشن‌هایی کرده است که از نظر آنان کاربران را مورد تهدید قرار داده‌اند. این اپلیکیشن‌ها هرکدام عموما دارای نقص‌های امنیتی می‌باشند که موجب آسیب پذیری کاربران ویا سو استفاده از آنان می‌شود.

این غول نرم افزاری این بار نیز تصمیم گرفته است تا به حذف اپلیکیشن‌هایی کند که دارای نقص امنیتی هستند اما این بار با کمی تفاوت. این بار از توسعه دهندگان آنان در طی فرآیندی خودکار خواسته شده تا هرچه زودتر این نقص‌ها را برطرف نمایند. که در ادامه‌ی این خبر به طور کامل توضیح داده خواهد شد.

یکی از اولویت‌های اصلی گوگل، حفظ امنیت کاربرانش می‌باشد. این امر منجر به حذف یک میلیون اپلیکیشن از Play Store شده است.

گوگل، این غول تکنولوژی، اخیرا یک میلیون اپلیکیشن را به دلیل نقص امنیتی از مارکت خود حذف نموده است تا با جدیت بیشتری، امنیت کاربرانش را پیگیری کند.

طبق گفته‌ی سخنگوی این شرکت: برنامه ارتقاع سطح امنیتی اپلیکیشن (ASIP) این شرکت به بیش از ۳۰۰۰۰۰ توسعه دهنده برای درست کردن ۱۰۰۰۰۰۰ اپلیکیشن در Google Play کمک کرده است. در سال ۲۰۱۸ به تنهایی، این برنامه به ۳۰۰۰۰ توسعه دهنده برای درست کردن ۷۵۰۰۰ اپلیکیشن کمک کرده است. این بدین معنی است که حداقل این ۷۵۰۰۰ اپلیکیشن به دلیل نقص امنیتی در Store پخش نشدند که این امر یک موفقیت بزرگ است.

گوگل برنامه امنیتی خود را برای بهبود وضع امنیتی برنامه‌ها به یک روال روتین تبدیل کرده است که اپلیکیشن‌هایی که دارای هیچ مشکل امنیتی نیستند، تست‌های نرمال برروی آن انجام شده و پس از آن برروی Google Play Store انتشار می‌یابند.

اما اگر یک اپلیکیشن داری نقص امنیتی باشد گوگل از انتشار آن خودداری می‌کند و به توسعه دهنده‌ی آن توصیه‌های لازم داده می‌شود.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATOR CENTER

مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.