کد خبر: ۱۰۰۵۸۶۰
دوشنبه ۳۰ اردیبهشت ۱۳۹۸ ۱۶:۳۰

رفع چهار نقص اجرای کد راه‌دور اندرویددر وصله‌ی امنیتی ماه می سال ۲۰۱۹ گوگل

وصله‌های امنیتی منتشرشده توسط گوگل در ماه می سال ۲۰۱۹، ۸ آسیب‌پذیری بحرانی در سیستم‌عامل ، از جمله ۴آسیب‌پذیری‌اجرای کد راه‌دور را برطرف می‌سازد.

به گزارش گروه علم و فناوری ایسکانیوز، وصله‌های امنیتی منتشرشده توسط گوگل در ماه می سال ۲۰۱۹، ۸ آسیب‌پذیری بحرانی در سیستم‌عامل ، از جمله ۴ آسیب‌پذیری اجرای کد راه‌دور را برطرف می‌سازد.

شدیدترین نقص رفع‌شده در این به‌روزرسانی، یک اشکال بحرانی در است که ممکن است از راه دور بااستفاده از یک فایل ساختگی خاص برای اجرای کد دلخواه در محدوده‌ی فرایند مجاز، مورد سواستفاده قرار گیرد. این آسیب‌پذیری با شناسه‌ی ۲۰۴۴–۲۰۱۹– ردیابی می‌شود و نسخه‌های ۷.۰، ۷.۱.۱، ۷.۱.۲، ۸.۰، ۸.۱و ۹ از سیستم‌عامل اندروید را تحت‌تأثیر قرار می‌دهد و در تمام دستگاه‌هایی که سطح وصله امنیتی ۰۱–۰۵–۲۰۱۹ را اجرا می‌کنند، برطرف شده است.

آسیب‌پذیری‌های بحرانی دیگری که در این سطح وصله برطرف شده‌اند شامل ۳ نقص اجرای کد راه دور (۲۰۴۶–۲۰۱۹– ،۲۰۴۵–۲۰۱۹– و ۲۰۴۷–۲۰۱۹–) در سیستم هستند. این نقص‌ها، نسخه‌های ۷.۰، ۷.۱.۱، ۷.۱.۲، ۸.۰، ۸.۱و ۹ از سیستم‌عامل اندروید را تحت‌تأثیر قرار می‌دهند.

پنج آسیب‌پذیری دیگری که در به‌روزرسانی ماه می سال ۲۰۱۹ برطرف شده‌اند شامل دو نقص افزایش امتیاز (۲۰۱۹– ،۲۰۴۹–۲۰۱۹– ۲۰۵۰) و سه نقص افشای اطلاعات (۲۰۵۲–۲۰۱۹– ،۲۰۵۱–۲۰۱۹– و ۲۰۵۳–۲۰۱۹–) هستند. تمامی این پنج آسیب‌پذیری از نظر شدت، بالا رتبه‌بندی شده‌اند.

سطح وصله امنیتی ۰۱–۰۵–۲۰۱۹ یک نقص افزایش امتیاز با شدت متوسط در را نیز برطرف می‌سازد. این نقص که با شناسه–۲۰۱۹– ۲۰۴۳ ردیابی می‌شود، می‌تواند یک برنامه‌ی کاربردی مخرب محلی را قادر سازد نیازمندی‌های تعامل کاربر را به‌منظور دست‌یافتن به مجوزهای بیشتر، دور بزند.

بخش دوم مجموعه وصله‌های اندرویدی ماه می سال ،۲۰۱۹ مسائل مربوط به اجزای ، اجزای ، اجزای و اجزای متن بسته‌ی ((– را برطرف می‌سازد. این آسیب‌پذیری‌ها در تمامی دستگاه‌هایی که سطح وصله امنیتی ۰۵–۰۵–۲۰۱۹ را اجرا می‌کنند، برطرف شده‌اند. این نقص‌ها شامل یک اشکال افزایش امتیاز با شدت متوسط در اجزای ، یک مشکل افزایش امتیاز با شدت بالا در اجزای و یک آسیب‌پذیری اجرای کد راه دور با شدت بالا در اجزای هستند. دو نقص برطرف‌شده در اجزای از نظر شدت، بالا رتبه‌بندی شده‌اند و ۱۵ نقص بطرف شده، مربوط به اجزای متن بسته‌ی هستند که ۴ مورد از آن‌ها بحرانی و ۱۱ مورد دیگر بالا رتبه‌بندی شده‌اند. چهار آسیب‌پذیری بحرانی در اجزای متن‌بسته‌ی ، با شناسه‌ی ۲۲۵۵–۲۰۱۹– ،۱۳۸۹۸–۲۰۱۸– ،۵۹۱۲–۲۰۱۸– و ۲۲۵۶–۲۰۱۹– ردیابی می‌شوند.

همانند چندین ماه گذشته، بولتین به‌روزرسانی برای ماه می سال ۲۰۱۹، شامل هیچگونه وصله امنیتی نیست. هیچ وصله‌ی عملکردی نیز برای این دستگاه‌ها منتشر نشده است. با این حال، دستگاه‌های یک به‌روزرسانی دریافت خواهند کرد که اصلاحات مربوط به مسائل بولتن امنیتی ماه می سال ۲۰۱۹ اندروید را ارائه خواهد کرد.

با انتشار بولتین‌های امنیتی گوگل، دارندگان گوشی‌های گوگل می‌توانند آن را به سرعت دریافت کنند؛ اما دریافت به‌روزرسانی امنیتی برای کاربران اندرویدی گوشی‌های هوشمند سایر فروشندگان ممکن است چندین ماه طول بکشد. این امر، یک وضعیت گیج‌کننده و نارضایتمندانه است که گوگل چندین سال است سعی دارد آن را برطرف سازد و اخیراً توضیح داده است که چگونه می‌خواهد این مسائل را در نسخه‌ی بعدی (در حال حاضر با عنوان) بهبود بخشد. در حال حاضر، به‌روزرسانی امنیتی از طریق سازندگان تلفن همراه، به صورت

به‌روزرسانی‌هایی که مختصات عناصر هر مدل و فروشنده را شامل می‌شود، دریافت می‌شود. ناگزیر، این امر زمان‌بر است.
با توجه به جزئیات منتشر شده در کنفرانس توسعه ۲۰۱۹ / و در مصاحبه‌ای با ، پروژه اصلی این شرکت برای ، یک رویکرد کاملاً متفاوت است که یک لیست از ۱۴ ماژول را هوایی (--) مستقیماً از به‌روزرسانی می‌کند. این ماژول‌ها عبارتند از:

ورود به پورتال

برطرف‌کننده‌ی

کدک‌های
اجزای
پیکربندی مجوز شبکه
اجزای شبکه‌سازی
کنترل‌گر مجوز
داده‌های
ابرداده‌های ماژول
به عبارتی دیگر، به‌روزرسانی این عناصر، مستقیماً از ، بدون هر گونه واسطی، صورت خواهد گرفت.

انتهای پیام/