بسمه تعالی

بررسی دو آسیب‌پذیری بحرانی در برنامه ایمیل اپل

گزارش آسیب‌پذیری

برنامه ایمیل پیش‌فرض از پیش نصب شده بر روی میلیون‌ها گوشی یا تبلت اپل نسبت به دو نقص بحرانی که مهاجمان حداقل از دو سال قبل برای جاسوسی قربانیان مشهور از آن استفاده می‌کنند، آسیب‌پذیر شده است.

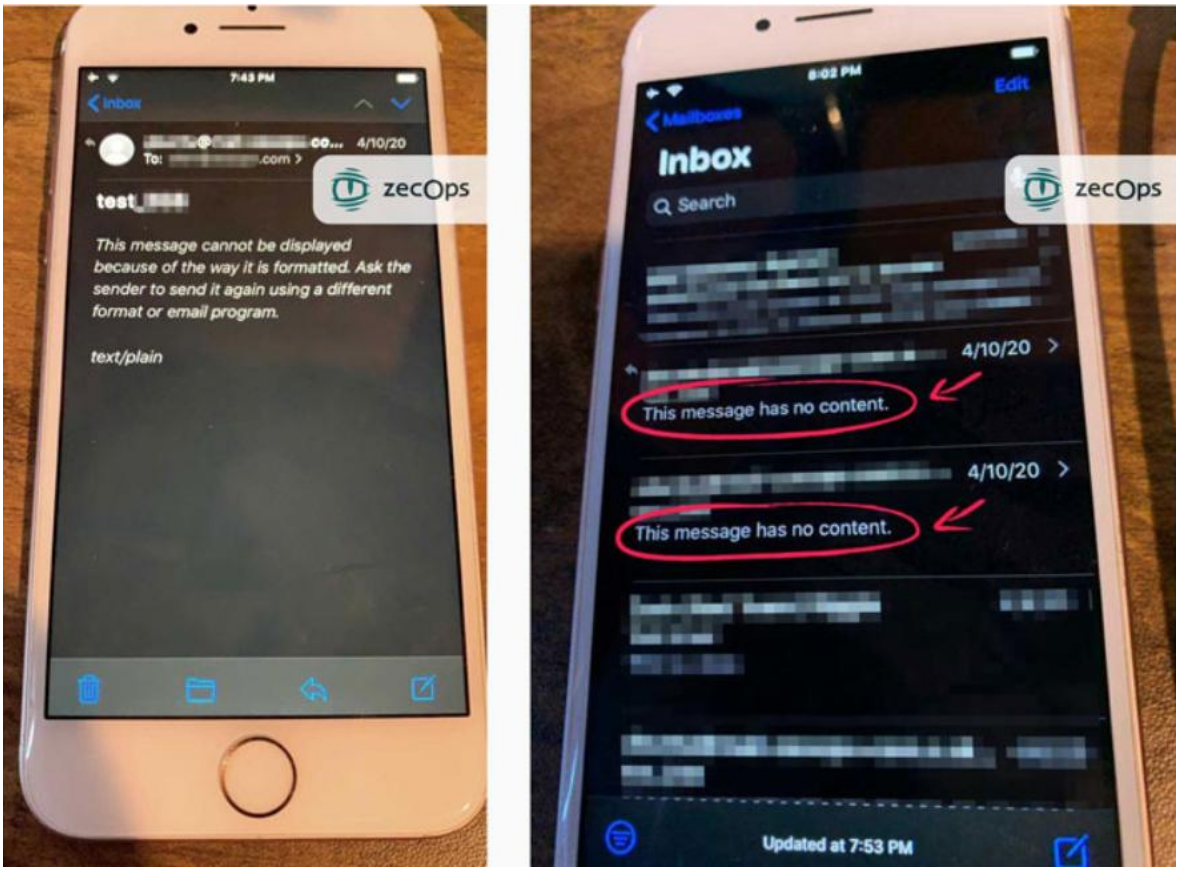
این نقص‌ها به مهاجمان از راه دور اجازه می‌دهند که تنها با فرستادن ایمیل به دستگاه‌های شخصی مورد نظر از طریق حساب ایمیل که در برنامه ایمیل آسیب‌پذیر وارد شده است، کنترل کاملی بر روی دستگاه‌های اپل به دست آورند.

طبق نظرات محققان در ZecOps آسیب‌پذیری‌های مورد نظر، نقص‌های اجرای کد از راه دور هستند که به دلایل باگ نوشتن خارج از محدوده[1] و مسئله سرریز پشته، در کتابخانه MIME برنامه ایمیل اپل اتفاق می‌افتند. اگرچه هر دو نقص هنگام پردازش محتوای ایمیل ایجاد می‌شوند، اما نقص دوم خطرناک‌تر است؛ زیرا می‌تواند بدون کلیک مورد بهره‌برداری قرار گرفته و نیاز به تعامل با گیرندگان هدف ندارد.

۱ جزئیات آسیب‌پذیری

نقص‌های موجود در مدل‌های مختلف گوشی و تبلت‌های اپل به مدت حداقل ۸ سال و از زمان انتشار iOS ۶ وجود داشته و همچنین روی iOS ۱۳,۴,۱ تأثیر گذاشته‌اند. تاکنون هیچ‌گونه وصله یا به‌روزرسانی برای این آسیب‌پذیری‌ها منتشر نشده است. چندین گروه از مهاجمان از حداقل دو سال پیش در حال سوءاستفاده از این نقص‌های روز صفرم به منظور هدف گرفتن اشخاص در صنایع و سازمان‌های مختلف، MSSPهای عربستان سعودی و اسرائیل و روزنامه‌نگاران در اروپا هستند. با وجود داده‌های محدود، حداقل ۶ سازمان تحت تأثیر این آسیب‌پذیری قرار گرفتند. دامنه سوءاستفاده کامل از این آسیب‌پذیری بسیار زیاد است. این حملات توسط یک عامل خاص صورت نمی‌گیرند و برخی از سازمان بهره‌برداری از آسیب‌پذیری‌هایی که از آدرس ایمیل به عنوان شاخص اصلی استفاده می‌کند را خرید و فروش می‌کنند.

[1] out-of-bounds write



شکل ۱: حمله به دستگاه‌های iOS از طریق برنامه‌های ایمیل

این آسیب‌پذیری بلافاصله پس از به دست آوردن کنترل کامل بر دستگاه، ایمیل مخرب را حذف می‌کند؛ بنابراین ممکن است برای کاربران اپل دشوار باشد که بدانند آیا به عنوان بخشی از این حملات سایبری هدف قرار گرفته‌اند یا خیر. طبق آمارها ایمیل‌های بهره‌برداری توسط دستگاه iOS قربانیان دریافت و پردازش شده و ایمیل‌های مربوطه که باید پس از دریافت در سرور ایمیل ذخیره می‌شدند، وجود نداشتند. بنابراین، درمی‌یابیم که این ایمیل‌ها به عنوان بخشی از اقدامات پاکسازی امنیتی حمله حذف شده‌اند. علاوه بر کندی موقت یک برنامه ایمیل تلفن همراه، کاربران نباید رفتار غیر عادی دیگری را مشاهده کنند.

لازم به ذکر است در صورت بهره‌برداری موفقیت آمیز، این آسیب‌پذیری با استفاده از برنامه MobileMail یا maild، کد مخرب را اجرا کرده و به مهاجمان اجازه می‌دهد ایمیل‌های خود را نشت، اصلاح و حذف کنند.

با این حال برای ایجاد کنترل کامل از راه دور بر روی دستگاه، مهاجمان باید این آسیب‌پذیری را با یک آسیب‌پذیری جداگانه اصلی ترکیب کنند. گروه ZecOps جزئیاتی در مورد اینکه مهاجمان از چه نوعی از بدافزار برای قربانیان استفاده می‌کنند، منتشر نکرده و معتقد است مهاجمان برای جاسوسی موفقیت‌آمیز از قربانیان خود، از ترکیب نقض‌ها با سایر نقض‌های اصلی استفاده می‌کنند.

۲ انتشار وصله

محققان نقض‌های در حال بهره‌برداری و نقض‌های مرتبطی با آن را دو ماه قبل کشف کرده و به گروه امنیتی اپل گزارش دادند. نسخه ۱۳,۴,۵ beta از iOS در هفته قبل منتشر شد و شامل وصله‌هایی امنیتی برای هر دو آسیب‌پذیری روز صفرم ذکر شده است. همچنین یک وصله نرم‌افزاری در به‌روزرسانی‌های آینده برای میلیون‌ها کاربر گوشی‌ها و تبلت‌های اپل منتشر خواهد شد. در همین حال به کاربران اپل توصیه می‌شود به جای استفاده از برنامه‌های ایمیل داخلی اپل، موقتاً از برنامه‌های Outlook یا Gmail استفاده کنند.

۳ مراجع

[۱] https://thehackernews.com/۲۰۲۰/۰۴/zero-day-warning-its-possible-to-hack.html