وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

بسمه تعالی

توصیه‌های ارتقاء امنیت برای توزیع کنندگان برنامه‌های سامانه‌های هوشمند همراه

معاونت امنیت فضای تولید و تبادل اطلاعات

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

سرفصل مطالب

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مقدمه

با توجه به استفاده روزافزون از سامانه‌های هوشمند همراه در بین اقشار مختلف جامعه و قابلیت‌های بسیاری که دستگاه‌های تلفن همراه در اختیار کاربران قرار می‌دهند، تضمین امنیت سامانه‌های هوشمند همراه حائز اهمیت است. یکی از مواردی که امنیت سامانه‌های هوشمند همراه را به مخاطره می‌اندازد، درگاه های عرضه و توزیع برنامک‌ها است. فروشگاه‌های برنامک نقش مهمی را در تضمین امنیت گوشی‌های هوشمند ایفا می‌کنند و در صورت رعایت توصیه های امنیتی می‌توانند از کاربران در مقابل توسعه‌دهندگان بدافزارها و برنامک های ناامن محافظت کنند. برای این منظور، ضروری است تا توصیه های امنیتی برای این بخش از زیست‌بوم برنامک‌ها شناسایی شوند. در این سند، توصیه های امنیتی به منظور مقابله با ریسک‌های امنیتی مطرح در زیست‌بوم برنامک‌ها و در جهت حفظ امنیت و حریم خصوصی استفاده کنندگان در حوزه بازارهای توزیع برنامک‌های گوشی‌های هوشمند تدوین شده‌اند. در این راستا، بر اساس توصیه‌های مطرح‌شده از سوی استانداردهای معتبر جهانی بررسی‌های لازم بر روی توصیه های امنیتی برای توزیع‌کنندگان برنامک‌های سامانه‌های هوشمند همراه صورت گرفته و به طور خلاصه و متناسب با شرایط حاکم بر فضای مجازی داخل کشور ارایه شده است.

۱ اختصارات و تعاریف

«**فروشگاه برنامک**»[۱] به توزیع‌کنندگان یا بازارهایی گفته می‌شود که برنامک‌ها را به صورت رایگان یا برای فروش به کاربران عرضه می‌کنند. فروشگاه برنامک، مخزنی مدیریت‌شده از نرم‌افزارهای شخص ثالث[۲] است. فروشگاه برنامک فرصت مناسبی را در اختیار توسعه‌دهندگان قرار می‌دهد تا به بازار برنامک‌های گوشی‌های هوشمند ورود کرده و کسب درآمد کنند. توسعه‌دهندگان می‌توانند با استفاده از پنجره‌ی مخصوصی که فروشگاه در اختیار آن‌ها قرار می‌دهد، برنامک‌های خود را منتشر، به‌روزرسانی و مدیریت کنند.

---

[۱] App Store

[۲] Third party

عموما، فروشگاه‌های برنامک به چهار دسته «**فروشگاه برنامک خارجی غیررسمی**»، «**فروشگاه برنامک خارجی رسمی**»، «**فروشگاه برنامک داخلی**» و «**فروشگاه برنامک سازمانی**» تقسیم‌بندی شده‌اند که عبارتند از[۳]:

- **فروشگاه برنامک خارجی غیررسمی** به فروشگاهی خارج از مرزهای جغرافیایی کشور گفته می‌شود که توسط یک واحد مستقل مدیریت می‌شود و تحت کنترل سازنده گوشی تلفن همراه یا یک سازمان و کسب‌وکار قرار ندارد. در بسیاری از موارد، جهت نصب برنامک‌های عرضه‌شده در این فروشگاه‌ها، لازم است که گوشی تلفن همراه محدودیت‌زدایی[۴] شود. به این ترتیب، نصب برنامک از طریق این فروشگاه‌ها می‌تواند خطرات امنیتی متعددی به دنبال داشته باشد. به عنوان نمونه‌هایی از این فروشگاه‌ها می‌توان به Cydia store، Mobile۱ ، AndroidPit، AndroidTap، Cadengo، PandaApp اشاره کرد.
- **فروشگاه برنامک خارجی رسمی** به فروشگاهی گفته می‌شود که به جهت موقعیت جغرافیایی خارج از محدوده کشور است و توسط سازنده سخت‌افزار یا توسعه‌دهنده سیستم‌عامل مدیریت می‌شود. این فروشگاه‌ها برای ارائه برنامک‌های تلفن همراه به عموم کاربران در سراسر دنیا در نظر گرفته شده‌اند. به عنوان مثال، می‌توان به فروشگاه برنامک آمازون[۵]، فروشگاه برنامک اپل، دنیای بلک‌بری[۶]، فروشگاه گوگل پلی[۷]، دنیای هوشمند ال‌جی[۸]، برنامک‌های سامسونگ[۹] و فروشگاه ویندوز فون[۱۰] متعلق به شرکت مایکروسافت اشاره کرد.

---

[۳] توضیح: در این مستند، تمرکز بر ارایه توصیه های به فروشگاه‌های برنامک داخلی است.

[۴] root or jailbreak

[۵] Amazon Appstore

[۶] BlackBerry World

[۷] Google Play Store

[۸] LG Smart World

[۹] Samsung Apps

[۱۰] Windows Phone Store

- **فروشگاه برنامک داخلی** به فروشگاه شخص ثالثی گفته می‌شود که در داخل کشور راه‌اندازی شده است و تحت کنترل شرکت‌های سازنده گوشی تلفن همراه قرار ندارد. کلیه فروشگاه‌های برنامک داخلی موظف به رعایت توصیه های مندرج در این سند و اخذ مجوز از مراجع ذی‌صلاح هستند.
- **فروشگاه برنامک سازمانی** به فروشگاهی گفته می‌شود که توسط سازمان‌ها (شرکت‌ها و سازمان‌های خصوصی و دولتی) راه‌اندازی شده است و منحصراً توسط کاربران مجاز سازمان مورد استفاده قرار می‌گیرد. کاربران مجاز در فروشگاه برنامک سازمانی متشکل از کارکنان خود سازمان و همچنین پیمانکاران و شرکای سازمان (کارکنان مربوط به سازمان‌های دیگر که با سازمان مربوطه همکاری می‌کنند) یا مشتریان آنها هستند. یک سازمان ممکن است نیاز داشته باشد که انواع متفاوتی از فروشگاه‌های برنامک را جهت پشتیبانی از گروه‌های مختلف کاربران در دامنه‌های امنیتی مختلف (همانند کاربران خارجی و کاربران مجاز) راه‌اندازی کند.

برای بیان دقیق توصیه های معرفی‌شده در این سند، لازم است که کلمات کلیدی تعریف شوند. بر مبنای توصیه **RFC ۶۹۱۹**، کلمات کلیدی «ضروری است»[۱۱]، «باید در نظر گرفته شود»[۱۲]، «می‌تواند»[۱۳] و «غیرقابل اعمال» برای بیان توصیه های در نظر گرفته شده‌اند. چهار کلمه کلیدی که در این سند از آن‌ها استفاده شده‌اند، در **جدول ۱** ارائه شده است.

جدول ۱. تعریف کلمات کلیدی براساس توصیه RFC ۶۹۱۹

قابل چشم‌پوشی	رنگ سفید: مخاطب توصیه موظف به اجرای توصیه نیست.
می‌تواند	رنگ سبز: عبارت «می‌تواند» در توصیه های به صورت یک «پیشنهاد» یا «تذکر» بیان می‌شود که بدون اعمال سخت‌گیرانه، یک عملکرد مطمئن و امن را ارائه می‌دهد. در این صورت، خود مخاطبین توصیه می‌توانند برای اعمال توصیه مورد نظر تصمیم بگیرند، هر چند بهتر است که توصیه را رعایت کنند.

[۱۱] Must

[۱۲] Should Consider

[۱۳] Could

باید در نظر گرفته شود	رنگ زرد: نویسندگانی که مشخصات توصیه را بیان می‌کنند، در خصوص مکانیسم دقیق انجام توصیه مطمئن نیستند. مخاطبان توصیه اغلب به علت عدم بلوغ فناوری، محدودیت‌های هزینه یا زمان می‌توانند از مکانیسم‌های اجرایی مختلف استفاده کنند، لذا اجرای این مجموعه از توصیه های اجباری است؛ اما هیچ‌گونه اجباری در خصوص نحوه انجام و مکانیسم اجرایی آن وجود ندارد.
ضروری است	رنگ قرمز: عبارت «ضروری است» برای بیان توصیه ای استفاده می‌شود که در راستای برآوردن نیازمندی‌ها قطعیت دارد (همانند مکانیسم‌های امنیتی ملزم-به-پیاده‌سازی). این عبارت زمانی به کار می‌رود که نویسندگان توصیه در مورد نحوه انجام (مکانیسم پیاده‌سازی) آن توصیه اطمینان کامل دارند. کاربرد این عبارت در خصوص توصیه هایی است که انجام دادن آن اجباری است.

۲ تهدیدات توزیع برنامه‌ها

تهدید عامل بالقوه‌ای است که از آسیب پذیری‌های موجود در سامانه ها استفاده می‌کند تا بتواند مقاصد مورد نظر حمله کننده را برآورده سازد. از این رو با استفاده از مدل‌سازی تهدید، مخاطرات مربوط به زیست‌بوم برنامک‌ها استخراج شده‌اند. این مخاطرات در جدول ۲ ارایه شده اند.

جدول ۲. مخاطرات مطرح در توزیع برنامک‌ها

کد مخاطره	عنوان مخاطره	شرح کنش مخاطره
R۱	دور زدن فروشگاه برنامک	در این مخاطره، مهاجم اقدام به دور زدن فروشگاه برنامک رسمی کرده و برنامک‌های خود را از طریق فروشگاه‌های غیرمجاز (یا منابع تأیید نشده) عرضه می‌کند. پس از آن فعالیت‌های غیرمجاز همانند افزودن برنامک‌های مخرب و روت کیت به فروشگاه غیررسمی را انجام می‌دهد.

R۲	سوءاستفاده از آسیب‌پذیری‌های موجود در برنامک‌های نصب‌شده	در صورت وجود آسیب‌پذیری در برنامک‌های نصب‌شده، مهاجم اطلاعات حساس (همانند مشخصات کاربرانی که اقدام به نصب برنامک کرده‌اند، اطلاعاتی که مشخص می‌کنند کدام برنامک‌ها روی کدام دستگاه نصب شده‌اند و همچنین اطلاعات مربوط به دستگاهی که کاربر مورد استفاده قرار می‌دهد) را به دست می‌آورد.
R۳	تبدیل برنامک‌ها به برنامک‌های مخرب	در این مخاطره فقط تهدیدات مربوط به اجرای برنامک مورد توجه قرار می‌گیرند، زیرا در اغلب موارد، رفتار مخرب در زمان اجرا پدیدار می‌شود. در این نوع تهدیدات، مهاجم فرایند اجرای برنامک را جعل یا دست‌کاری کرده و یا روی فرایند اجرا سربار اعمال کرده تا اقدام به انجام عملیات مخرب کند.
R۴	دور زدن فرایند بررسی[۱۴] برنامک‌ها	در این مخاطره، مهاجم تهدیداتی را اعمال کرده و فرایند بررسی برنامک را دور می‌زند. رفتارهای پرخطر از سوی توسعه‌دهندگان شناخته‌شده می‌تواند نشانه‌ای از یک حمله (همانند حمله فیشینگ) باشد.
R۵	تحریف اعتبار برنامک‌ها	مهاجم چندین هویت مستعار برای خود ایجاد کرده و با به دست آوردن نفوذ زیاد، اعتبار برنامک ارائه‌شده در فروشگاه را تحریف می‌کند (با این هدف که اعتبار بیشتری را برای برنامک‌ها نشان دهد).
R۶	ممانعت از تشخیص توسط کاربر	در این مخاطره، مهاجم از طریق اعمال سربار روی فروشگاه برنامک یا جعل فروشگاه برنامک، از اینکه کاربران بتوانند نظرات و شکایات خود را ثبت کنند یا توضیحات مربوط به برنامک را مشاهده کنند، ممانعت می‌کنند.
R۷	ممانعت از دریافت به‌روزرسانی‌ها و امحاء برنامک	مهاجم از طریق انجام فعالیت‌های مخرب مانع از دریافت به‌روزرسانی‌ها یا امحاء مربوط به برنامک‌های نصب‌شده روی دستگاه کاربر می‌شود.

[۱۴] Review

۳ جایگاه

توصیه های معرفی شده در این سند، در راستای اقدام ۲-۱ از راهبرد دوم سند راهبردی افتا، با عنوان ایجاد و توسعه نظام‌های فرابخشی افتا و چارچوب توصیه های امنیتی شبکه ملی اطلاعات قرار دارند.

۴ اهداف

- کمک به حفظ امنیت و حریم خصوصی کاربران
- ارتقای سطح حفاظت از اسرار کسب‌وکار سازمانی/حاکمیتی/خصوصی
- پیش‌گیری از مخاطرات در توزیع برنامک‌های سامانه‌های هوشمند همراه
- انتظام بخشی و تقویت صنعت و ارایه خدمات در زیست‌بوم سامانه‌های هوشمند همراه

۵ ذینفعان و مخاطبین

- کاربران سامانه‌های هوشمند همراه
- اپراتورهای تلفن همراه
- توسعه‌دهندگان برنامک‌ها
- توزیع‌کنندگان برنامک‌ها
- سیاست‌گذاران سازمانی
- سازندگان سامانه‌های هوشمند همراه

۶ توصیه های امنیتی

در این بخش توصیه های امنیتی مربوط به فروشگاه‌های برنامک در جدول ۳ ارایه شده‌اند. علاوه بر تعریف توصیه سطح اعمال به انواع فروشگاه نیز ذکر شده است. برای این منظور از کلمات کلیدی تعریف‌شده در **جدول ۱** برای مشخص کردن سطح رعایت توصیه استفاده شده است. لازم به ذکر است که تعدادی از توصیه های معرفی‌شده قادر هستند که چندین مخاطره را به طور همزمان پوشش دهند و برای پیشگیری از تکرار آنها اجتناب شده است. کد توصیه Ri-j اشاره به توصیه زام برای مخاطره Ri در جدول ۲ را دارد.

جدول ۳. توصیه های امنیتی فروشگاه‌های توزیع برنامک

ردیف	کد توصیه	شرح توصیه
۱	توصیه R۱-۱	فروشگاه‌های برنامک در راستای اعتلای امنیت برنامک‌ها در کشور، با اعلام توافق روی مواردی از جمله حداقل سطح توصیه‌شده برای امنیت، به تشکیل ائتلاف[۱۵] و توافق با سایر فروشگاه‌ها مبادرت کنند.
سطح اعمال	داخلی (می‌تواند)	
۲	توصیه R۱-۲	فروشگاه برنامک، مکانیسمی را به کار گیرد که به کاربران اجازه دهد مشروعیت[۱۶] فروشگاه را شناسایی کنند.
سطح اعمال	داخلی (ضروری)	
۳	توصیه R۱-۳	کلیه فروشگاه‌های برنامک از مرکز توسعه تجارت الکترونیکی وزارت صنعت، معدن و تجارت برای وب‌سایت خود نماد «اعتماد الکترونیکی» اخذ کنند.
سطح اعمال	داخلی (ضروری)	
۴	توصیه R۱-۴	فروشگاه برنامک از ارایه برنامک‌هایی که نیاز به محدودیت‌زدایی(jailbreak کردن یا root کردن) دارند خودداری نماید.
سطح اعمال	داخلی (ضروری)	

[۱۵] Federation

[۱۶] Legitimate

ردیف	کد توصیه	شرح توصیه
۵	توصیه R۱-۵	فروشگاه برنامک از ارائه آموزش‌های مرتبط با محدودیت‌زدایی (jailbreak کردن یا root کردن) سامانه های هوشمند همراه خودداری کند.
سطح اعمال	داخلی (ضروری)	
۶	توصیه R۱-۶	فروشگاه برنامک در بخش راهنمای نصب برنامک‌ها یا در صفحه اول وب‌سایت خود، کاربران را از خطرات امنیتی مربوط به نصب برنامک‌ها از منابع ناشناخته[۱۷] آگاه کند.
سطح اعمال	داخلی (ضروری)	
۷	توصیه R۱-۷	فروشگاه برنامک قبل از عرضه برنامک‌ها به کاربران نهایی، آن‌ها را با استفاده از ابزارهای تحلیل امنیتی و بر اساس چک لیست مصوب و حداقل‌های امنیتی درنظر گرفته شده (چک لیست پیوست و جدول ۴)، بررسی و مستندکند. به علاوه فروشگاه دستورالعملی مدون در خصوص رعایت حداقل‌های امنیتی لازم برای برنامک‌ها داشته باشد.
سطح اعمال	داخلی (ضروری)	
۸	توصیه R۱-۸	فروشگاه برنامک نتایج تجزیه و تحلیل‌های امنیتی خود در مورد برنامک‌ها را با سایر فروشگاه‌های برنامک و محققین امنیتی به اشتراک بگذارد.
سطح اعمال	داخلی (می‌تواند)	

[۱۷] Unknown Sources

ردیف	کد توصیه	شرح توصیه
۹	توصیه R۱-۹	فروشگاه برنامک، توسعه‌دهندگان برنامک‌ها را از نظر امنیتی احراز اصالت کند تا توسعه‌دهندگان جعلی نتوانند از اسم و رسم و اعتبار (خوب) توسعه‌دهندگان دیگر سوء استفاده کنند.
سطح اعمال	داخلی (ضروری)	
۱۰	توصیه R۱-۱۰	فروشگاه برنامک برای هر یک از توسعه‌دهندگان برنامک یک پروفایل امنیتی ایجاد کند و ریسک‌های ایجادشده از سوی آنها را به دقت رصد کند.
سطح اعمال	داخلی (ضروری)	
۱۱	توصیه R۱-۱۱	فروشگاه برنامک اعتبار توسعه‌دهندگان برنامک‌ها را بررسی کند.
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۱۲	توصیه R۱-۱۲	فرایند بررسی برنامک یک فرایند مستمر باشد و فروشگاه باید برنامک را حتی پس از اینکه (توسط فروشگاه) مورد پذیرش قرار گرفت نیز به طور دوره‌ای(۶ ماهه) تحلیل یا رصد امنیتی کند.
سطح اعمال	داخلی (ضروری)	
۱۳	توصیه R۱-۱۳	فروشگاه برنامک، به‌روزرسانی‌های برنامک‌های به روز شده موجود در فروشگاه و تحلیل امنیتی مجدد آنها را حداکثر ۳ روز پس از دریافت آخرین نسخه یا وصله از توسعه

ردیف	کد توصیه	شرح توصیه
		دهندگان برنامک انجام داده و سپس به روزرسانی برنامک را به اطلاع مشتریان خود برساند.
سطح اعمال	داخلی (ضروری)	
۱۴	توصیه R۱-۱۴	فروشگاه برنامک توسعه‌دهندگان را ملزم کند که برنامک‌های خود را جهت پذیرش در فروشگاه به صورت دیجیتالی امضا نمایند.
سطح اعمال	داخلی (ضروری)	
۱۵	توصیه R۱-۱۵	فروشگاه برنامک بررسی کند که مجوزهای دسترسی درخواست‌شده توسط هر برنامک با اهداف آن برنامک تناقضی نداشته باشد.
سطح اعمال	داخلی (ضروری)	
۱۶	توصیه R۱-۱۶	فروشگاه برنامک بررسی کند که تمامی برنامک‌ها لیست مجوزهای دسترسی مورد نیاز خود را در زمان نصب نمایش می‌دهند.
سطح اعمال	داخلی (ضروری)	
۱۷	توصیه R۱-۱۷	فروشگاه برنامک راهنماها و دستوالعمل‌هایی[۱۸] امنیتی را جهت کمک به توسعه‌دهندگان برای تولید و ارائه برنامک‌هایی مطابق با قوانین تعیین‌شده از سوی فروشگاه و نهادهای ذیصلاح، برای رعایت حداقل‌های امنیتی ارائه دهند.

[۱۸] Guidelines

ردیف	کد توصیه	شرح توصیه
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۱۸	توصیه R۱-۱۸	فروشگاه برنامک، سیاست‌ها، قوانین و شرایطی را که در ارتباط با امنیت و حریم خصوصی وضع کرده است، به تأیید نهادهای ذی‌صلاح برساند (در صورت وجود چنین نهادهایی) و پس از اعلام عمومی قوانین در سایت فروشگاه، بدون تأیید نهادهای مربوطه اقدام به تغییر آن‌ها ننماید.
سطح اعمال	داخلی (ضروری)	
۱۹	توصیه R۱-۱۹	فروشگاه برنامک در خصوص استفاده غیرقانونی از برنامک‌های موجود در فروشگاه، هشدارهایی را به کاربران اعلام کند.
سطح اعمال	داخلی (ضروری)	
۲۰	توصیه R۱-۲۰	فروشگاه برنامک، برای خدمات پرداخت‌های درون‌برنامکی یک کتابخانه تهیه کند و آن را در اختیار توسعه‌دهندگان قرار دهد، یا استفاده از کتابخانه‌های مورد تایید نهادهای ذیصلاح بانکی را به آنها توصیه نماید.
سطح اعمال	داخلی (ضروری)	
۲۱	توصیه R۱-۲۱	فروشگاه برنامک بر تبلیغات درون‌برنامکی برنامه‌های فروشگاه، مطابق قوانین و سیاست‌های کشور نظارت داشته و در این خصوص دستورالعمل داشته باشد.

ردیف	کد توصیه	شرح توصیه
سطح اعمال	داخلی (ضروری)	
۲۲	توصیه R۱-۲۲	فروشگاه برنامک از انتشار برنامک‌هایی که از بستر USSD برای انجام تراکنش‌های مالی خود استفاده می‌کنند، خودداری کند.
سطح اعمال	داخلی (ضروری)	
۲۳	توصیه R۱-۲۳	فروشگاه برنامک، آموزش‌ها و اطلاع‌رسانی‌های مرتبط با امنیت سیستم‌عامل، امنیت برنامک‌ها یا آلوده شدن سامانه‌های هوشمند همراه به انواع بدافزارها و نرم‌افزارهای مخرب را در وب‌سایت یا ویترین خود قرار دهد.
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۲۴	توصیه R۱-۲۴	فروشگاه برنامک پیش از انتشار برنامک ها آنها را از نظر وجود بدافزار، آزمون و ارزیابی نماید و از انتشار برنامک های حاوی بدافزار جلوگیری نماید. همچنین پس از کسب اطلاع از وجود بدافزار در برنامک‌ها سریعا آنها را از ویترین فرشگاه خارج نماید.
سطح اعمال	داخلی (ضروری)	
۲۵	توصیه R۱-۲۵	فروشگاه برنامک پیش از انتشار برنامک‌هایی که نیاز به دریافت مجوز از نهادهای مربوطه دارند، از وجود این مجوزها اطمینان حاصل نماید.
سطح	داخلی	

ردیف	کد توصیه	شرح توصیه
اعمال	(ضروری)	
۲۶	توصیه R۱-۲۶	فروشگاه برنامک مکانیسم‌هایی را جهت تعیین و نمایش اعتبار برنامک‌ها و توسعه‌دهندگان آن‌ها در نظر بگیرد (دستورالعمل داشته باشند).
سطح اعمال	داخلی (ضروری)	
۲۷	توصیه R۱-۲۷	فروشگاه برنامک اعتبار سنجی مجزایی را در خصوص رتبه امنیتی و حریم خصوصی برنامک‌های عرضه شده در نظر بگیرد.
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۲۸	توصیه R۱-۲۸	فروشگاه برنامک، نظرات و شکایات کاربران سامانه‌های هوشمند همراه در خصوص برنامک‌ها را با رعایت حفظ حریم خصوصی کاربران در تحلیل امنیتی برنامک ها دخالت داده، آرشیو نموده و یا به صورت عمومی نمایش دهد.
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۲۹	توصیه R۱-۲۹	فروشگاه برنامک، تبادل اطلاعات مرتبط با اعتبار برنامک‌ها با سایر فروشگاه‌های برنامک را مد نظر قرار دهد.
سطح اعمال	داخلی (می‌تواند)	

ردیف	کد توصیه	شرح توصیه
۳۰	توصیه R۱-۳۰	فروشگاه برنامک به منظور عرضه کلیه خدمات خود، اقدام به پیاده‌سازی بستر ثبت‌نام و ایجاد حساب کاربری برای کاربران و توسعه‌دهندگان کند.
سطح اعمال	داخلی (ضروری)	
۳۱	توصیه R۱-۳۱	فروشگاه برنامک امکان مشاهده رتبه‌بندی، امتیازات و نظرات کاربران بر روی برنامک‌ها را برای توسعه‌دهندگان برنامک ها فراهم نماید.
سطح اعمال	داخلی (ضروری)	
۳۲	توصیه R۱-۳۲	فروشگاه برنامک محرمانگی و حریم خصوصی اطلاعات دریافتی از سوی کاربران و توسعه‌دهندگان برنامک‌ها (همچون نام، نام خانوادگی، شماره تلفن همراه، شماره ملی و شماره حساب بانکی) را حفظ کند.
سطح اعمال	داخلی (ضروری)	
۳۳	توصیه R۱-۳۳	فروشگاه برنامک به منظور حفظ کیفیت نظرات ثبت‌شده از سوی کاربران، آن‌ها را پس از بازبینی و تأیید انسانی نمایش دهد.
سطح اعمال	داخلی (می‌تواند)	
۳۴	توصیه R۱-۳۴	فروشگاه برنامک جهت انجام تراکنش‌های مالی (دریافت هزینه از کاربران و توسعه‌دهندگان برنامک) تمامی جوانب یک پرداخت ایمن را در نظر بگیرد (دستورالعمل داشته باشد).

ردیف	کد توصیه	شرح توصیه
سطح اعمال	داخلی (ضروری)	
۳۵	توصیه R۱-۳۵	فروشگاه برنامک مکانیسم امحاء برنامک را پیاده‌سازی کند (که به این روش kill-switch نیز گویند).
سطح اعمال	داخلی (باید در نظر گرفته شود)	
۳۶	توصیه R۱-۳۶	فروشگاه برنامک کاربران خود را تشویق کند که به طور مستمر به‌روزرسانی‌های[۱۹] مربوط به برنامک‌های به روز شده و نصب‌شده روی سامانه هوشمند همراه خود را انجام دهند.
سطح اعمال	داخلی (ضروری)	
۳۷	توصیه R۱-۳۷	فروشگاه برنامک تا حدی که امکان دارد، وصله‌ها و به‌روزرسانی‌های امنیتی برنامک‌ها را در اندازه‌های کوچک ارائه کند.
سطح اعمال	داخلی (می‌تواند)	
۳۸	توصیه R۱-۳۸	فروشگاه برنامک با هدف تشخیص برنامک‌هایی که باید امحاء شوند یا از فروشگاه خارج شوند، نظرات و شکایات کاربران را به صورت مستمر تحت نظارت قرار دهد.
سطح	داخلی	

[۱۹] Update

ردیف	کد توصیه	شرح توصیه
اعمال	(ضروری)	
۳۹	توصیه R1-۳۹	فروشگاه برنامک ضمن داشتن دستورالعمل، از کارشناسان امنیتی برای مکانیسم امحاء برنامک‌ها در سطوح مختلف (فروشگاه، توسعه دهنده، مشتری، سامانه) استفاده نماید.
سطح اعمال	داخلی (ضروری)	
۴۰	توصیه R1-۴۰	فروشگاه برنامک در صورت مشاهده تخلف توسط یک توسعه‌دهنده برنامک (همانند سوء استفاده از اطلاعات کاربران، کپی کردن برنامک یک توسعه‌دهنده دیگر، تقلب و دستکاری در امتیازدهی برنامک و ثبت نظرات خلاف واقع)، نسبت به حذف برنامک متخلف از ویترین فروشگاه اقدام کرده و جلوی کلیه دسترسی‌های داده‌شده به آن توسعه‌دهنده را بگیرد و یا در صورت لزوم موضوع را با سایر فروشگاه‌ها یا نهادهای ذیصلاح به اشتراک بگذارد.
سطح اعمال	داخلی (ضروری)	
۴۱	توصیه R1-۴۱	فروشگاه برنامک در صورت دریافت درخواست از سوی یک توسعه‌دهنده در خصوص حذف برنامک از ویترین فروشگاه، این کار را با تأیید تیم امنیتی فروشگاه انجام دهد.
سطح اعمال	داخلی (ضروری)	
۴۲	توصیه R1-۴۲	فروشگاه برنامک درخصوص به روز رسانی برنامک‌ها و نحوه اطلاع رسانی به مشتریان دستورالعمل داشته و با توسعه دهندگان برنامک‌ها توافق نامه داشته باشد.

رد یف	کد توصیه	شرح توصیه
سطح اعمال	داخلی (ضروری)	

۷ پیوست ۱: چک‌لیست توصیه های امنیتی برای برنامک‌های موبایل بر اساس OWASP

در طی «فرایند بررسی» یا «فرایند پذیرش یک برنامک از توسعه دهنده» لازم است توزیع‌کننده به ازای هر برنامک، چک‌لیست جدول ۴ را مد نظر قرار دهد. این چک‌لیست امنیتی برای برنامک‌های سامانه های هوشمند همراه توسط OWASP معرفی شده است. این چک لیست باید هر شش ماه یا بسته به ضرورت در زمان کمتر از شش ماه مورد بازبینی قرار گیرد. جدول آزمون‌های مختلفی را نشان می‌دهد که فروشگاه برنامک باید قبل از انتشار هر برنامک، این آزمون‌ها را بر روی آن به انجام برساند. بدین منظور، برنامک‌ها به دو دسته **عام** و **خاص** تقسیم بندی شده‌اند. برنامک‌های عام برنامک‌هایی هستند که نیازمندی امنیتی آنها در سطح پایین تری نسبت به برنامک-های خاص قرار دارد. از این رو، آزمون‌های امنیتی کمتری برای آنها در نظر گرفته شده است. به عنوان نمونه، برنامک‌هایی مانند ویرایش اسناد، بازی‌های ساده و به طور کلی برنامک‌هایی که از پروتکل‌های امنیتی استفاده نمی‌کنند و مستقیما با مسایل محرمانگی و حریم خصوصی کاربر ارتباط ندارد در دسته برنامک‌های عام قرار می-گیرند. همچنین برنامک‌هایی که در حوزه‌های بانکی، سلامت و غیره هستند یا برنامک‌هایی که از پروتکل‌های امنیتی استفاده می‌کنند و مستقیم یا غیر مستقیم با مسایل محرمانگی و حریم خصوصی کاربر ارتباط دارند در دسته برنامک‌های خاص گنجانده می‌شوند. در جدول دو ستون مجزا برای هریک از این دو نوع برنامک در نظر گرفته شده است. در هر ستون هم آزمون‌هایی که باید به ازای آن نوع برنامک انجام شوند، مشخص شده‌اند.

فروشگاه برنامک باید به ازای هر برنامک دریافتی، آن برنامک را در یکی از دو دسته عام یا خاص قرار دهد و بر اساس جدول زیر، آزمون‌های امنیتی را روی آن انجام دهد و برنامک‌ها باید در آزمون‌ها با توجه به ستون عام یا خاص با موفقیت قبول شوند. نتیجه آزمون‌ها باید در یک پرونده امنیتی که مختص هر برنامک ایجاد می‌شود، به

طور دقیق و معتبر درج شود. همچنین، به ازای تمامی وصله های ارائه شده به ازای آن برنامک باید آزمون‌ها از ابتدا انجام شوند تا اطمینان حاصل شود که آن وصله مشکل امنیتی ندارد. پس از انجام آزمون‌های امنیتی، فروشگاه برنامک باید با توجه به نتایج به دست آمده، اقدام به انتشار یار رد برنامک نماید. این موضوع شامل کلیه برنامک‌های داخلی و خارجی می‌شود. به علاوه جدول ارتباط هر آزمون امنیتی با ۱۰ مخاطرات برتر امنیتی OWASP برای گوشی‌های هوشمند همراه را نشان می‌دهد. جهت اطلاع، کلیه آزمون‌های مندرج در جدول بر اساس اسناد OWASP در [۱] پیشنهاد شده اند. جزییات مربوط به نحوه انجام هر آزمون و ابزار مورد نیاز در سند مذکور قابل ملاحظه است. همچنین نوع آزمون (ایستا یا پویا) به صورت یک ستون مجزا در جدول قرار داده شده است.

جدول ۴ چک لیست امنیت برنامک‌های تلفن همراه

ردیف	نوع آزمون	هدف و شرح آزمون	آزمون عام	آزمون خاص	انطباق؟ بله/خیر/NA	OWASP Mobile Top ۱۰	متد آزمون
۱	آزمون ذخیره داده‌ها						
۱-۱	آزمون داده‌های حساس در قسمت ذخیره‌سازی محلی	عدم ذخیره داده‌های حساس (مانند کلیدهای رمزنگاری) در حافظه داخلی یا خارجی در محل‌های زیر: • Shared Preferences • SQLite Databases	✓	✓		M۱ M۲	تحلیل ایستا + پویا
۱-۲	آزمون داده‌های حساس در لاگ فایل‌ها	عدم لاگ برداری از داده‌های حساس (مانند نام کاربری یا sessionID) در زمان اشکال‌زدایی برنامک‌ها.	✓	✓		M۱ M۲	تحلیل ایستا + پویا
۱-۳	آزمون فرستادن داده حساس به شخص سوم	ناتوانی در سوء استفاده از داده‌های حساسس توسط سرویس‌های شخص سوم درون برنامک‌ها.	✓	✓		M۱ M۲	تحلیل ایستا + پویا
۱-۴	آزمون اینکه آیا کش کی‌برد برای متن ورودی[۲۰] غیرفعال است	غیرفعال بودن حافظه صفحه کلید هنگام ورود اطلاعات حساس (مانند پسورد یا اطلاعات بانکی) و ارائه پیشنهاد در متن ورودی.	✓	✓		M۱ M۲	تحلیل ایستا + پویا
۱-۵	آزمون داده‌های حساس در کلیپ بورد	غیرفعال بودن کلیپ بورد در زمان وارد کردن اطلاعات حساس (مانند پسورد یا اطلاعات بانکی).	✓	✓		M۱ M۲	تحلیل ایستا + پویا
۱-۵	آزمون اینکه آیا داده‌های حساس از طریق مکانیزم‌های IPC افشاء می‌شوند	عدم نشت اطلاعات از طریق مکانیزم‌های IPC مانند: • Binders	✓	✓		M۱ M۲	تحلیل ایستا +

[۲۰] Inter-Process Communication

		• Services
		  ○ Bound Services
		  ○ AIDL
		• Intents
		• Content Providers
							پویا

۱-۷	آزمون اینکه آیا داده‌های حساس از طریق واسط کاربری افشاء می‌شوند	ناتوانی در تصویربرداری از صفحه برنامک‌ها مثلا وقتی که برنامکی باز است و حاوی اطلاعات حساسی مانند شماره حساب است.	✓	✓		M۴	تحلیل ایستا + پویا
۲	**آزمون رمزنگاری**						
۲-۱	وارسی مدیریت کلید	عدم استفاده از کلیدهای رمزنگاری قابل خواندن (چه در داخل کد برنامه و چه در فایل‌ها یا دیگر فضاهای ذخیره‌سازی)	-	✓		M۶	تحلیل ایستا
۲-۲	آزمون پیاده‌سازی‌های سفارشی در رمزنگاری	استفاده از الگوریتم‌های رمزنگاری استاندارد و غیر قابل شکستن (به این معنی که هنوز روشی برای شکستن سریع آن‌ها ارائه نشده باشد).	-	✓		M۶	تحلیل ایستا
۲-۳	وارسی پیکربندی الگوریتم‌های استاندارد رمزنگاری	پیکربندی مناسب الگوریتم‌های رمزنگاری.	-	✓		M۶	تحلیل ایستا + پویا
۲-۴	آزمون الگوریتم‌های رمزنگاری ناامن و/یا منسوخ	استفاده از الگوریتم‌های رمزنگاری قوی و بهره‌مندی از توصیه های امنیتی مدرن رمزنگاری.	-	✓		M۶	تحلیل ایستا
۲-۵	آزمون تولید عدد تصادفی	عدم استفاده از عدد تصادفی قابل حدس.	-	✓		M۶	تحلیل ایستا
۳	**آزمون احراز اصالت و مدیریت جلسه**						
۳-۱	وارسی صحت احراز اصالت کاربران	بررسی پیروی مکانیسم احراز اصالت از استانداردهای موجود. برای مثال: احراز اصالت کاربر از طریق سرور خارجی و نه در داخل دستگاه.	✓	✓		M۴	تحلیل ایستا + پویا

۳-۲	آزمون مدیریت جلسه[۲۱]	بررسی رعایت استانداردهای امنیتی برای مدیریت جلسات برای مثال: اطمینان از وجود زمان انقضا برای جلسه	-	✓		M۴	تحلیل + ایستا + پویا
۳-۳	آزمون عملکرد خروج	بررسی رعایت توصیه های امنیتی در زمان پایان یک جلسه	-	✓			
۳-۴	آزمون سیاست کلمه عبور	رعایت حداقل توصیه های در سیاست کلمه عبور.	✓	✓		M۴	تحلیل + ایستا + پویا
۳-۵	آزمون تلاش بیش از اندازه برای ورود	برنامک کنترلی برای جلوگیری از دسترسی بیش از تعداد تعریف شده برای ورود به سیستم داشته باشد. (جلوگیری از حمله brute force)	✓	✓		M۴	تحلیل + ایستا + پویا
۳-۶	آزمون احراز اصالت بیومتریک	استفاده از الگوریتم‌های استاندارد در احراز اصالت بیومتریک (در صورت وجود)	-	✓		M۴	تحلیل + ایستا + پویا
۳-۷	آزمون پیاده سازی اتمام مهلت جلسه	پیاده‌سازی اتمام خودکار جلسه، به خصوص در برنامک‌هایی که با داده‌های حساس سروکار دارند مهم است.	-	✓		M۴	تحلیل + ایستا + پویا
۳-۸	آزمون احراز اصالت دو فاکتوری	استفاده از مکانیزم احراز اصالت به صورت دوفاکتوری.	-	✓		M۴	تحلیل + ایستا + پویا
۴	**آزمون ارتباطات شبکه**						
۴-۱	آزمون داده‌های حساس رمزنگاری نشده روی شبکه	استفاده از مکانیزم‌های رمزنگاری برای جلوگیری از شنود داده‌های حساس بر روی شبکه و حملات مرد میانی.	✓	✓		M۳	تحلیل + ایستا + پویا
۴	آزمون تنظیمات TLS	استفاده از کلید و رمزنگاری	-	✓		M۳	تحلیل

[۲۱] Session

۲-		استاندارد و قوی در پروتکل TLS.					پویا
۴ ۳-	آزمون شناسایی نقطه پایانی	لازم است تا دو پارامتر «زنجیره گواهی» و «نام میزبان» مربوط به سرور، در برنامک به درستی اعتبارسنجی شوند.	-	✓		M۳	تحلیل ایستا + پویا
۴ ۴-	آزمون گواهی سفارشی و SSL Pinning	تکنیک ssl pinning گواهی سرور در برنامک موبایل زمانی پیاده‌سازی می‌شود، که برنامک تنها به تعداد محدودی سرور قابل اعتماد متصل شود. در این حالت لازم است تا گواهی آن سرورها به‌صورت دستی در کد برنامک قرار گرفته باشد.	-	✓		M۳	تحلیل ایستا + پویا
۴ ۵-	وارسی اینکه عملیات بحرانی از کانال‌های ارتباطی امن استفاده می‌کند	عدم استفاده از کانال‌های ارتباطی ناامن (مانند SMS برای ثبت نام کاربران یا بازیابی اطلاعات) یا افزودن مکانیزم امنیتی پیشرفته به آن‌ها در صورت استفاده از این کانال‌ها.	✓	✓		M۳	تحلیل ایستا + پویا
۵	**آزمون تعامل پلتفرم**						
۵ ۱-	آزمون مجوزهای برنامک	عدم استفاده برنامک از مجوزهای حساس یا بیش از حد نیاز.	✓	✓		M۱	تحلیل ایستا + پویا
۵ ۲-	آزمون طرح URL سفارشی	در زمان تعامل بین برنامک‌ها، برنامک نباید قابلیت حساس را از طریق طرح URL سفارشی صادر نماید، مگر اینکه مکانیزم‌های آن محافظت شده باشند.	✓	✓		M۱	تحلیل ایستا + پویا
۵ ۳-	آزمون اجرای جاوا اسکریپت در WebView	اگر در پیاده‌سازی WebView اجازه استفاده از جاوا اسکریپت داده شود، نباید بتوان از جاوا اسکریپت برای حمله به برنامک استفاده کرد و امکان دسترسی به داده‌ها را به دست آورد.	-	✓		M۷	تحلیل ایستا + پویا

۵ ۴-	آزمون رسیدگی‌کننده[۲۲] پروتکل WebView	چندین طرح موجود به‌طور پیش‌فرض در اندروید که می‌تواند توسط WebView راه‌اندازی می‌شوند: - http(s) - file - tel - geo باید جلوی دسترسی غیرمجاز به پروتکل‌های مذکور از طریق WebView گرفته شده باشد.	✓	✓		M۷	**تحلیل ایستا + پویا**
۵ ۵-	آزمون تغییر فایل‌های محلی در WebView	فایل‌های محلی در پوشه داده برنامک یا حافظه خارجی می‌توانند توسط WebView بارگذاری شوند. کاربر نباید توانایی تغییر در نام یا مسیر و تدوین این فایل‌ها را داشته باشد.	✓	✓		M۷	**تحلیل ایستا + پویا**
۵ ۶-	آزمون امنیت مکانیزم Serialization	در صورت استفاده از Serialization جاوا نباید نتیجه به صورت خام در فایل ذخیره شده یا بر روی شبکه ارسال شود؛ بلکه باید رمزنگاری شده و امنیت آن تضمین شده باشد.	✓	✓		M۷	**تحلیل ایستا**
۶	**آزمون کیفیت کد و ساخت تنظیمات**						
۶ ۱-	وارسی اینکه آیا برنامک به‌درستی امضاء شده است	امضاء برنامک شامل پروسه‌ای است که گواهی کلید عمومی به apk متصل می‌شود. در این آزمون بررسی می‌شود که برنامک‌ها از گذرواژه‌های قوی برای کلید خصوصی و keystore استفاده کرده و تنظیمات فایل‌ها و اطلاعات امضاء را نشت ندهند.	✓	✓		M۷	**تحلیل ایستا**

[۲۲] Handlers

[۴] Debug

۶-۲	آزمون اینکه آیا برنامک قابل اشکال‌زادیی[۴] است	لازم است قابلیت اشکال‌زدایی برنامک برای کاربران غیر فعال باشد	-	✓		Mv	**تحلیل ایستا**
۶-۳	آزمون برای سمبل‌های اشکال‌زادیی	در وارسی جدول‌های سمبل، نباید سمبل‌های اشکال‌زادیی دیده شود.	-	✓		Mv	**تحلیل ایستا + پویا**
۶-۴	آزمون رسیدگی خطا	وارسی اینکه برنامک اطلاعات حساس را هنگام رسیدگی به خطا فاش نسازد.	-	✓		Mv	**تحلیل ایستا**
۶-۵	وارسی اینکه امکانات امنیتی در زمان کامپایل فعال شده‌اند	از آنجا که دی‌کامپایل کردن کلاس‌های جاوا کار نسبتا ساده‌ای است، لازم است از مبهم‌سازی استفاده شده باشد.	-	✓		Mv	**تحلیل ایستا + پویا**

منبع:

[۱] https://b-mueller.gitbooks.io/owasp-mobile-security-testing-guide/content/۰x۰۳-Overview.html