وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

بررسی نقاط ضعف و آسیب‌پذیری‌های سیستم‌های عامل استفاده‌شده در تلویزیون‌های هوشمند موجود در ایران

مرکز ماهر

شماره نگارش 4/0

طبقه‌بندی ..... عادی

تابستان 1396

بررسی نقاط ضعف و آسیب‌پذیری‌های سیستم‌های عامل استفاده‌شده در تلویزیون‌های هوشمند موجود در ایران

فهرست مطالب

فهرست شکل‌ها

فهرست جداول

1- مقدمه

سیستم‌های عامل پرکاربرد در صنعت تلویزیون‌های هوشمند موجود در بازار ایران، سیستم‌های عامل WebOS، اندروید با نسخه‌های 4.2.1 ، 4.4 ، 4.4.2، 4.4.4 و 5.1 و سیستم عامل تایزن 2.4 می‌باشند. شرکت معروف LG به‌عنوان یکی از پیشگامان حوزه تلویزیون‌های هوشمند از سیستم‌عامل WebOS بهره می‌برد. WebOS سیستم‌عاملی چندوظیفه‌ای مبتنی بر هسته لینوکس برای دستگاه‌های هوشمند مثل تلویزیون‌های هوشمند می‌باشد و به عنوان سیستم‌عامل موبایل استفاده شده است. توسعه اولیه بوسیله Palm بوده و HP پلت‌فرم را منبع‌باز ساخته که با نام Open WebOS شناخته شد. در جدول 1، تلویزیون‌های مختلف موجود در بازار ایران که از سیستم‌عامل WebOS استفاده می‌کنند، ذکر شده است. لیست تلویزیون‌های موجود در بازار ایران از طریق جستجو در بازار و لیست تلویزیون‌های موجود در فروشگاه‌های اینترنتی بدست آمده است و از هیچ منبع خاصی استفاده نشده است.

جدول 1- تلویزیون‌های مختلف موجود در بازار ایران با سیستم عامل WebOS

شرکت	محصول	سیستم‌عامل
LG	LG Signature OLED G6	WebOS 3.0
LG	LG OLED E6	WebOS 3.0
LG	LG OLED B6	WebOS 3.0

شرکت‌های زیادی به سیستم‌عامل اندروید با نسخه‌های متعدد روی آورده‌اند. اندروید سیستم‌عاملی رایج و معروف بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشد. در جدول 2 تلویزیون‌های مختلف موجود در بازار ایران که از سیستم‌عامل اندروید استفاده می‌کنند، ذکر شده است.

جدول 2- تلویزیون‌های مختلف موجود در بازار ایران با سیستم‌عامل اندروید

شرکت	محصول	سیستم‌عامل
Sony	Sony KD 55X8500D Smart BRAVIA Series LED TV	اندروید 5.1
Sony	Sony KDL 43W800C BRAVIA Series Smart LED TV	اندروید 5.1
Sony	Sony LED 4K TV 55X8500C	اندروید 5.1
TOSHIBA	TOSHIBA LED Smart TV 47L5450	اندروید 4.4
TOSHIBA	TOSHIBA Full HD 40L5550	اندروید 4.4.2
TOSHIBA	TOSHIBA Full HD LED TV 55L5550	اندروید 4.4.2
TOSHIBA	TOSHIBA Smart TV LED Full HD 50L5550	اندروید 4.4.2
XVision	XVision 50XS520S Smart LED TV	اندروید 4.2.1
XVision	XVision 55XK530S Smart LED TV	اندروید 4.4.4
Sharp	Sharp 50UE630X Forka Smart	اندروید 5.1
Sharp	Sharp 58UE630X ULTRA HD	اندروید 5.1
Snowa	Snowa SLD-43S44BLD Smart LED TV	اندروید 5.1
Snowa	Snowa Smart SLD-50S44BLD	اندروید 5.1

سیستم‌عامل تایزن، سیستم‌عاملی می‌باشد که توسط سامسونگ مورد استفاده قرار گرفت تا بر روی دستگاه‌های ساخت سامسونگ نصب گردد. از آنجایی‌که نتوانست در مقابل اندروید مقاومت کند، جز موارد اندکی در کشورهای مورد درخواست، بازار تلفن‌های همراه هوشمند را از دست داده و از این رو گوشی‌های سامسونگ اغلب با سیستم‌عامل اندروید عرضه می‌گردند. سامسونگ، سیستم‌عامل تایزن را بر روی سایر لوازم خانگی از جمله تلویزیون‌های هوشمند و یخچال‌های هوشمند(جدیداً)، عرضه کرد. در جدول 3، تلویزیون‌های مختلف موجود در بازار ایران که از سیستم‌عامل تایزن استفاده می‌کنند، ذکر شده است.

جدول 3- تلویزیون‌های مختلف موجود در بازار ایران با سیستم عامل تایزن

شرکت	محصول	سیستم‌عامل
Samsung	Samsung 78KS9995	تایزن 2.4
Samsung	Samsung 65MS9995	تایزن 2.4
Samsung	Samsung 65KS8985	تایزن 2.4
Samsung	Samsung 70KU7970	تایزن 2.4

در بخش‌های بعد، سیستم‌های عامل پرکاربرد در تلویزیون‌های هوشمند موجود در ایران بررسی‌شده و آسیب‌پذیری‌های هر یک گزارش می‌گردد. همچنین مدل‌هایی از تلویزیون‌های هوشمند موجود در ایران که از آن سیستم‌عامل‌ها بهره می‌برند، نیز گزارش خواهد شد.

2- پارامترهای مطرح در ارزیابی آسیب‌پذیری‌ها

پارامترهای مطرح در ارزیابی آسیب‌پذیری‌ها، محرمانگی[1]، صحت[2]، دسترس‌پذیری[3]، پیچیدگی دسترسی[4] می‌باشند. هریک از این پارامترها در ادامه بحث خواهند شد. همچنین هریک از سیستم‌های عامل رایج در تلویزیون‌های موجود در ایران، بحث‌شده و آسیب‌پذیری موجود در هریک، براساس پارامترهای مطرح‌شده در بخش‌های بعد، ارزیابی خواهند شد.

2-1- محرمانگی

محرمانگی یعنی اطلاعات به‌گونه‌ای باشد که توسط فرد مهاجم قابل استفاده نباشد. در مبحث آسیب‌پذیری، تاثیر هریک از آسیب‌پذیری‌ها بر روی محرمانگی برطبق سه سطح کیفی بی‌تاثیر، جزئی[5] و کامل[6] ارزیابی شده است. در سطح کیفی جزئی در مبحث محرمانگی، افشای اطلاعات در حد قابل توجهی وجود دارد و در سطح کیفی کامل، کل سیستم و فایل‌های سیستمی افشاء می‌گردد.

[1] Confidentiality
[2] Integrity
[3] Availibility
[4] Access Complexity
[5] Partial
[6] Complete

2-2- صحت

صحت، صحیح‌بودن اطلاعات و خطادار نبودن اطلاعات می‌باشد. یعنی اطلاعات به شکل درست به مقصد منتقل شده باشد. در مبحث آسیب‌پذیری، تاثیر هریک از آسیب‌پذیری‌ها بر روی صحت، برطبق سه سطح کیفی بی‌تاثیر، جزئی و کامل ارزیابی شده است. در سطح کیفی جزئی در مبحث صحت، برخی فایل‌های سیستمی یا اطلاعات ممکن است تغییر یابد ولی مهاجم بر روی چیزی که می‌تواند تغییر دهد، کنترل ندارد و حوزه چیزی که می‌تواند بر روی آن اثر بگذارد، محدود است. در سطح کیفی کامل در مبحث صحت، کل صحت سیستم به خطر می‌افتد و سیستم فاقد حفاظت می‌باشد.

2-3- دسترس‌پذیری

دسترس‌پذیری بیانگر میزان دسترس‌پذیر بودن سیستم برای استفاده می‌باشد. در مبحث آسیب‌پذیری، تاثیر هریک از آسیب‌پذیری‌ها بر روی دسترس‌پذیری، برطبق سه سطح کیفی بی‌تاثیر، جزئی و کامل ارزیابی شده است. در سطح کیفی جزئی در مبحث دسترس‌پذیری، کارایی منبع کاهش یافته و در دسترس‌پذیری منبع، وقفه ایجاد می‌شود. در سطح کیفی کامل در مبحث دسترس‌پذیری، منبع آلوده‌شده کاملاً خاموش‌شده و غیرقابل دسترس می‌گردد.

2-4- پیچیدگی دسترسی

پیچیدگی دسترسی، میزان پیچیده‌بودن دسترسی به آسیب‌پذیری برای بهره‌برداری از آن می‌باشد. در مبحث آسیب‌پذیری، تاثیر هریک از آسیب‌پذیری‌ها بر روی پیچیدگی دسترسی، برطبق سه سطح کیفی کم[۷]، متوسط[۸] و بالا[۹] ارزیابی شده است. در سطح کیفی کم در مبحث پیچیدگی دسترسی، مهارت و دانش خیلی کم برای بهره‌برداری از آسیب‌پذیری موردنیاز می‌باشد. در سطح کیفی متوسط در مبحث پیچیدگی دسترسی، مهارت و دانش در حد متوسط برای بهره‌برداری از آسیب‌پذیری لازم بوده و شرایط دسترسی خاص‌تر از حالت قبل می‌باشد. در سطح کیفی بالا در مبحث پیچیدگی دسترسی، شرایط دسترسی به‌گونه‌ای است که بهره‌برداری از آسیب‌پذیری خیلی سخت می‌باشد.

3- سیستم‌عامل WebOS

سیستم‌عامل WebOS شناخته‌شده با نام‌های Open WebOS یا LG WebOS (قبلاً با HP WebOS یا Palm WebOS شناخته می‌شد) سیستم‌عامل چندوظیفه‌ای[۱۰] مبتنی بر هسته لینوکس برای دستگاه‌های هوشمند مثل تلویزیون‌های هوشمند[۱۱] می‌باشد و به عنوان سیستم‌عامل موبایل[۱۲] استفاده شده است. این سیستم‌عامل ابتدا توسط Palm توسعه یافت و بعدها شرکت HP نسخه منبع‌باز آن را با نام Open WebOS منتشر کرد. این سیستم‌عامل بعداً به شرکت LG فروخته شد. نسخه‌های متنوعی از WebOS روی دستگاه‌های متنوعی مثل Pre، Pixi، Veer smartphones، TouchPad tablet و Smart TV از سال 2015 نصب شده است. پلت‌فرم موبایل WebOS برخی

[7] Low
[8] Medium
[9] High
[10] Multitask
[11] Smart TV
[12] Mobile Operating System

قابلیت‌های جدیدی از جمله قابلیت واسط card [۱۳] را معرفی کرد که هنوز در سیستم‌های عامل شرکت‌های Apple، Microsoft و Google به ترتیب iOS، Windows Phone و Android استفاده می‌شود[115].

3-1- پلت‌فرم

واسط کاربری گرافیکی[۱۴] WebOS اشتراک زیادی با توزیع‌های لینوکس دارد. نسخه‌های 1.0 تا 2.1 این سیستم‌عامل از هسته‌ی اصلاح‌شده لینوکس 2.6.24 استفاده می‌کنند[115].

3-2- آسیب‌پذیری[۱۵] سیستم‌عامل WebOS 3.0

آسیب‌پذیری‌های موجود در سیستم‌عامل WebOS 3.0 بر اساس پارامترهای مطرح در ارزیابی آسیب‌پذیری‌ها، در جدول 4 بیان شده‌اند.

جدول 4- آسیب‌پذیری‌های موجود در سیستم‌عامل WebOS 3.0

شماره شناسه	نام آسیب‌پذیری	نوع آسیب‌پذیری	محرمانگی	صحت	دسترس‌پذیری	پیچیدگی دسترسی	توضیحات	امتیاز از 10
CVE-2011-2409[1]	Cross-site scripting در برنامه تقویم	تزریق کد	بی‌تاثیر	جزئی	بی‌تاثیر	متوسط	احراز هویت[۱۶] نیاز نمی‌باشد	4.3
CVE-2011-2408[2]	Cross-site scripting در برنامه مخاطبین	تزریق کد	بی‌تاثیر	جزئی	بی‌تاثیر	متوسط	احراز هویت نیاز نمی‌باشد	4.3

3-1-7- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

در ایران دستگاه‌های استفاده‌کننده از سیستم‌عامل WebOS تلویزیون‌های هوشمند شرکت LG می‌باشند. LG به عنوان یکی از پیشگامان در ساخت تلویزیون‌های هوشمند است. تلویزیون‌های هوشمند LG Signature OLED G6، LG OLED E6، LG OLED B6، LG UHD، LG LED 55LH60000GI، LG LED 55LF65000GI از جمله تلویزیون‌های هوشمند موجود در بازار ایران هستند که مجهز به سیستم‌عامل WebOS 3.0 می‌باشند. این تلویزیون‌های هوشمند متاثر از آسیب‌پذیری‌های ذکرشده هستند.

4- سیستم‌عامل اندروید[۱۷]

اندروید سیستم‌عامل توسعه‌داده‌شده توسط شرکت گوگل[۱۸] براساس هسته لینوکس است و اساساً برای دستگاه‌های موبایل صفحه‌لمسی مثل تلفن‌های هوشمند[۱۹] و تبلت‌ها طراحی شده است. واسط کاربری اندروید براساس دستکاری مستقیم[۲۰] با استفاده از حرکات لمسی[۲۱] مناسب است که تناظر با فعالیت‌های دنیای واقعی مانند کشیدن و ضربه

[13] Card Interface
[14] Graphical User Interface
[15] Vulnerability
[16] Authentication
[17] Android
[18] Google
[19] Smartphones
[20] Direct Manipulation
[21] Touch Gestures

زدن[۲۲] برای دستکاری اشیای روی صفحه نمایش به همراه صفحه کلید مجازی برای ورودی متن، طراحی شده است. علاوه بر دستگاه‌های صفحه‌لمسی، گوگل AndroidTV را برای تلویزیون‌ها، Android Auto را برای اتومبیل‌ها وAndroid Wear را برای ساعت‌های مچی توسعه داده است که هریک واسط کاربری خود را دارا است. این سیستم‌عامل ابتدا توسط شرکت Android توسعه داده شد و سپس در سال 2005 توسط گوگل خریداری شد[116].

4-1- سخت‌افزار

پلت‌فرم سخت‌افزاری اندروید، ARM (با معماری‌های ARMv7 و ARMv8-A) با معماری‌های x86، MIPS و MIPS64 و x86-64 است. اندروید 4.4 نیازمند پردازنده ARMv7 32 بیتی با معماری MIPS یا x86 همراه با OpenGL ES2.0 سازگار با واحد پردازش گرافیکی[۲۳] (GPU) می‌باشد. اندروید از OpenGL ES 1.1,2.0,3.0,3.1 و نسخه‌های نهایی 3.2 و Vulkan پشتیبانی می‌کند. برخی از برنامه‌های کاربردی ممکن است بطور ضمنی نیازمند نسخه مشخصی از OpenGL ES و سخت‌افزار GPU، باشند[116] .

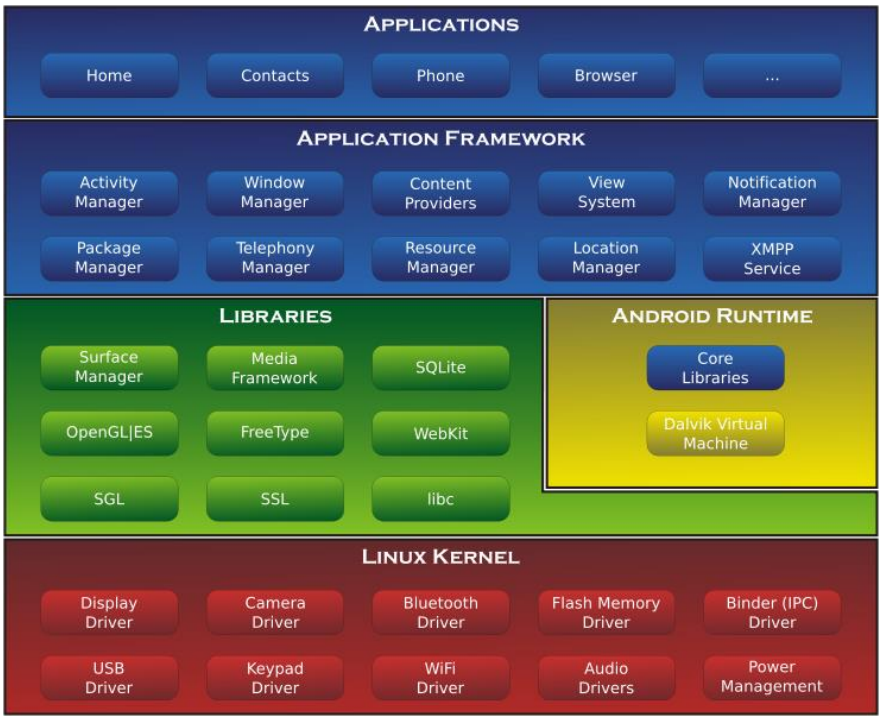
4-2- هسته لینوکس

هسته اندروید بر اساس بخش‌های پشتیبانی طولانی‌مدت[۲۴] (LTS) هسته لینوکس می‌باشد. از آپریل 2014، دستگاه‌های اندرویدی از نسخه‌های 3.4, 3.10 یا 3.18 هسته لینوکس، استفاده می‌کنند. اندروید از نسخه‌های مختلفی استفاده می‌کند. به عنوان مثال در اندروید 1.0 از نسخه 2.6.25 استفاده شده است[116].

4-3- پشته نرم‌افزاری[۲۵]

در بالای هسته لینوکس، میان‌افزار[۲۶]، کتابخانه‌ها و API های نوشته‌شده در C وجود دارند و نرم‌افزار برنامه کاربردی بر روی قالب‌کاری برنامه کاربردی اجراشده که شامل کتابخانه‌های سازگار با جاوا[۲۷] می‌باشد. معماری اندروید در شکل 1 نشان داده شده است[116].

[22] Tapping
[23] Graphics Processing Unit
[24] Long-term Support
[25] Software Stack
[26] Middleware
[27] Java-compatible



شکل 1- معماری اندروید [116]

با توجه به شکل 1 می‌توان گفت که در پایین‌ترین لایه، هسته لینوکس قرار دارد. راه‌انداز نمایشی[۲۸]،راه‌انداز دوربین[۲۹] و راه‌اندازهای دیگر در این لایه و در هسته لینوکس قرار دارند. لایه دوم از معماری اندروید، لایه کتابخانه‌ها و زمان‌اجرای اندروید[۳۰] می‌باشد. در بخش کتابخانه‌ها، مدیر سطح[۳۱]، قالب‌کاری رسانه[۳۲]، SQLite، OpenGL|ES، FreeType، Webkit، SGL، SSL و libc قرار دارد و در بخش زمان‌اجرای اندروید از لایه دوم، کتابخانه‌های هسته[۳۳] و ماشین مجازی Dalvik [۳۴] قرار دارد. لایه سوم از معماری اندروید، قالب‌کاری برنامه کاربردی می‌باشد که دارای مدیر فعالیت[۳۵]، مدیر پنجره[۳۶]، تامین‌کنندگان محتوا[۳۷]، سیستم نمایش[۳۸]، مدیر آگاه‌سازی[۳۹]، مدیر بسته[۴۰]، مدیر تلفن[۴۱]، مدیر منبع[۴۲]، مدیر مکان[۴۳] و سرویس XMPP می‌باشد. در لایه چهارم از معماری اندروید، برنامه‌های کاربردی نظیر خانه[۴۴]، مخاطبین[۴۵]، تلفن[۴۶]، مرورگر[۴۷] و غیره قرار دارند. تا نسخه 5، اندروید از Dalvik به عنوان یک

[28] Display Driver
[29] Camera Driver
[30] Android Runtime
[31] Surface Manager
[32] Media Framework
[33] Core Libraries
[34] Dalvik Virtual Machine
[35] Activity Manager
[36] Window Manager
[37] Content Providers
[38] View System
[39] Notification Manager
[40] Package Manager
[41] Telphony Manager
[42] Resource Manager
[43] Location Manager
[44] Home
[45] Contacts

ماشین مجازی پردازش به همراه کامپایل مبتنی بر ردیابی درجا[۴۸] (JIT) برای اجرای Dalvik dex-code (کدهای اجرایی Dalvik) استفاده می‌کند که معمولاً از بایت‌کد جاوا[۴۹] ترجمه شده است[116].

4-4- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.2.1

ارزیابی آسیب‌پذیری‌ها موجود در سیستم‌عامل اندروید 4.2.1 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم عامل، در صورتی که محرمانگی بی‌تاثیر باشد، در جدول 5 بیان شده است.

جدول 5- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.2.1 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0603[3]	Libstagefright	بی‌تاثیر	کامل	بالا	-منع سرویس -تعلیق[۵۰] /راه‌اندازی مجدد[۵۱] دستگاه	5.4
2017-0491[25]	ترفیع در حقوق در Package Manager	جزئی	بی‌تاثیر	متوسط	مانع کاربران از پاک‌کردن[۵۲] برنامه‌های کاربردی یا حذف مجوزها از برنامه	4.3
2017-0489[26]	ترفیع در حقوق در Location Manager	جزئی	بی‌تاثیر	متوسط	-رد نمودن حفاظت OS از داده محلی	4.3
2017-0422[32]	منع‌سرویس در Bionic DNS	بی‌تاثیر	کامل	کم	-استفاده از یک بسته شبکه مخدوش و تعلیق و راه‌اندازی مجدد دستگاه	7.8
2017-0395[41]	ترفیع در حقوق در Contacts	جزئی	بی‌تاثیر	متوسط	-ساخت اطلاعات مخاطب جدید - دسترسی به عملیاتی که ممکن است بطور معمول نیازمند مقداردهی اولیه یا اجازه کاربر باشد	4.3
2017-0393[43]	منع‌سرویس در libvpx	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2017-0390[44]	منع‌سرویس در Tremolo/dpen.s	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6766[47]	منع‌سرویس در libmedia	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6763[48]	منع‌سرویس در Telephony	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1

[46] Phone
[47] Browser
[48] Trace-based Just-in-time Compilation
[49] Java Bytecode
[50] Hang
[51] Reboot
[52] Uninstalling

2016-5348[53]	منع سرویس با استفاده از GPS توسط مهاجمین مردمیانی[۵۳]	بی‌تاثیر	کامل	متوسط	- مصرف حافظه و تعلیق یا راه اندازی مجدد دستگاه از طریق فایل xtra.bin یا xtra2.bin روی یک میزبان	7.1
2016-3881[61]	تابع decoder_peek_si_internal در vp9/vp9_dx_iface.c	بی‌تاثیر	کامل	متوسط	-منع‌سرویس (خواندن بیش از اندازه[۵۴]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3879[62]	arm-wt-22k/lib_src/eas_mdls.c	بی‌تاثیر	کامل	متوسط	- سبب منع‌سرویس (ارجاع اشاره‌گر تهی[۵۵]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3831[72]	منع سرویس با جز telephony	بی‌تاثیر	جزئی	کم	-کاربرد نادرست توسط ساعت سیستم و منع سرویس (خرابی دستگاه) از طریق مقدار زمانی NITZ 2038-01-19 یا بعدتر	5
2016-2495[81]	SampleTable.cpp	بی‌تاثیر	کامل	متوسط	- منع‌سرویس (تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل مخدوش	7.1
2016-2424[93]	SyncStorageEngine.java از SyncStorageEngine	بی‌تاثیر	کامل	متوسط	-مدیریت نادرست داده مرجع معین - منع‌سرویس (حلقه راه‌اندازی مجدد) از طریق برنامه کاربردی مخدوش	7.1
2016-0818[108]	کش‌سازی در کلاس TrustManagerImpl از TrustManagerImpl.java	جزئی	بی‌تاثیر	متوسط	-کاربرد نادرست تمایز مابین CA میانی و CA ریشه مطمئن - مهاجمین مرد میانی می‌توانند سرورها را بوسیله پوشش دسترسی به CA میانی، جعل نمایند	4.3

آسیب‌پذیری‌های موجود در سیستم عامل اندروید 4.2.1 با محرمانگی جزئی در جدول 6 بیان شده است.

جدول 6- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.2.1 با محرمانگی جزئی

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0602[4]	افشاء اطلاعات در بلوتوث	بی‌تاثیر	بی‌تاثیر	متوسط	-دورزدن حفاظت‌های OS توسط برنامه مخرب	4.3

[53] Man in the middle attackers
[54] Buffer over-read
[55] Null Pointer Reference

2017-0598[5]	افشای اطلاعات در قالب‌کاری[۵۶] API	بی‌تاثیر	بی‌تاثیر	متوسط	-دورزدن حفاظت‌های OS توسط برنامه مخرب	4.3
2017-0560[11]	افشای اطلاعات در پردازش بازگشت به تنظیمات کارخانه	بی‌تاثیر	بی‌تاثیر	متوسط	- ردشدن حفاظت دستگاه -دسترسی به داده صاحب قبلی	4.3
2017-0559[12]	افشای اطلاعات در libskia	بی‌تاثیر	بی‌تاثیر	متوسط	دسترسی به داده، بدون مجوز	4.3
2017-0558[13]	افشای اطلاعات در Mediaserver	بی‌تاثیر	بی‌تاثیر	متوسط	دسترسی به داده، بدون مجوز	4.3
2017-0554[14]	ترفیع در حقوق در جزء تلفن[۵۷]	جزئی	جزئی	متوسط	دستیابی به توانایی بدون مجوز	6.8
2017-0547[16]	افشای اطلاعات در libmedia	بی‌تاثیر	بی‌تاثیر	متوسط	- ردشدن حفاظت OS -دسترسی به داده، بدون مجوز	4.3
2017-0425[31]	افشای اطلاعات در Audioserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0420[34]	افشای اطلاعات در AOSP Mail	بی‌تاثیر	بی‌تاثیر	متوسط	-رد نمودن حفاظت OS	4.3
2017-0402[37]	افشای اطلاعات در EffectBundle.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0401[38]	افشای اطلاعات در EffectBundle.cpp از Qualcomm audio	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0396[40]	افشای اطلاعات در EffectVisualizer.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2016-6703[51]	اجرای کد راه دور در یک کتابخانه زمان اجرای اندروید	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-6702[52]	اجرای کد راه دور در libjpeg	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-3897[57]	کلاس WifiEnterpriseConfig در WifiEnterpriseConfig.java	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش و رمز عبور موجود در مقدار بازگشتی از متد فراخوانی (به صورت رشته از این کلاس)	4.3
2016-3896[58]	AOSP Mail و اطلاعات EmailAccountCacheProvider	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست‌آوردن اطلاعات از طریق برنامه کاربردی مخدوش	4.3
2016-3835[70]	نشست امن در جزء mm-video-v4l2 venc	بی‌تاثیر	بی‌تاثیر	متوسط	-استفاده نادرست از اشاره‌گرهای هیپ -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-3834[71]	camera APIs	بی‌تاثیر	بی‌تاثیر	متوسط	-رد نمودن محدودیت دسترسی -بدست‌آوردن اطلاعات حساس درباره آدرس‌های بافر ANW از طریق برنامه کاربردی مخدوش	4.3
2016-3822[73]	exif.c استفاده‌شده در libjhead	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (دسترسی خارج از	7.5

[56] Framework
[57] Telephony Component

	محدوده) از طریق داده EXIF مخدوش					
2016-3761[74]	NfcService.java در NFC	بی‌تاثیر	بی‌تاثیر	کم	-بدست‌آوردن اطلاعات برنامه کاربردی پیش‌زمینه[58] حساس از طریق برنامه کاربردی پس‌زمینه مخدوش	2.1
2016-3744[76]	سرریز بافر در create_pbuf function در btif/src/btif_hh.c در بلوتوث	جزئی	جزئی	بالا	-بدست‌آوردن حقوق از طریق عملیات جفت‌سازی مخدوش	4.3
2016-2499[80]	AudioSource.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-مقداردهی اولیه نادرست -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-2463[83]	سرریز عدد صحیح در جزء h264dec	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	7.5
2016-2426[92]	جزء قالب‌کاری ContentService.java	بی‌تاثیر	بی‌تاثیر	متوسط	-عدم بررسی جهت مجوز GET_ACCOUNTS -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-1155[99]	تزریق سرآیند Http در کلاس URLConnection	جزئی	جزئی	کم	-اجرای اسکریپت‌های دلخواه یا مقداردهی مقادیر دلخواه را در کوکی‌ها[59]	7.5
2016-0850[100]	PORCHE_PAIRING_CONFLIC در بلوتوث	جزئی	جزئی	کم	-ردنمودن محدودیت‌های جفت‌سازی از طریق دستگاه مخدوش	5.8
2016-0829[105]	BnGraphicBufferProducer.onTra در IGraphicBufferConsumer.cpp	بی‌تاثیر	بی‌تاثیر	کم	-عدم مقداردهی اولیه برای ساختارداده‌ای معین -بدست‌آوردن اطلاعات حساس -ردنمودن حفاظت بوسیله راه‌اندازی فعالیت QUEUE_BUFFER	5

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.2.1 با محرمانگی کامل در جدول 7 بیان شده است.

جدول 7- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.2.1 با محرمانگی کامل

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0596[6]	ترفیع در حقوق libstagefright	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز[60]	9.3

[58] Foreground
[59] Cookies
[60] Privileged Process

9.3	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن حقوق و دسترسی محلی	متوسط	کامل	کامل	SoftAACEncoder2.cpp	2017-0594[7]
9.3	-اجرای کد راه دور در داخل پردازش -خرابی حافظه در طول پردازش توسط فایل مخدوش	متوسط	کامل	کامل	FLACExtractor.cpp	2017-0592[8]
9.3	- اجرای کد راه دور در داخل پردازش -خرابی حافظه در طول پردازش توسط فایل مخدوش	متوسط	کامل	کامل	id3/ID3.cpp	2017-0588[10]
9.3	-بدست‌آوردن دسترسی به توانایی بدون مجوز -اجرای کد دلخواه در مفهوم پردازش ممتاز	متوسط	کامل	کامل	ترفیع در حقوق در SurfaceFlinger	2017-0546[17]
9.3	-اجرای کد دلخواه در مفهوم پردازش ممتاز	متوسط	کامل	کامل	ترفیع در حقوق در CameraBase	2017-0544[19]
9.3	- اجرای کد راه دور در داخل پردازش -خرابی حافظه در طول پردازش توسط فایل مخدوش	متوسط	کامل	کامل	اجرای کد راه دور در sonivox	2017-0541[20]
9.3	-اجرای کد دلخواه در پردازش ممتاز - بدست‌آوردن دسترسی به توانایی بدون مجوز	متوسط	کامل	کامل	ترفیع در حقوق در Audioserver	2017-0480[28]
9.3	-اجرای کد دلخواهی را در مفهوم هسته - احتمال خراب شدن دائمی دستگاه - پاک‌سازی و قرارگیری مجدد سیستم عامل برای ترمیم دستگاه	متوسط	کامل	کامل	ترفیع در حقوق در recovery verifier	2017-0475[30]
9.3	-اجرای کد دلخواه در پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	متوسط	کامل	کامل	ترفیع در حقوق در Audioserver	2017-0419[35]
9.3	-دسترسی به داده حساس بدون مجوز	متوسط	کامل	کامل	افشای اطلاعات در silk/NLSF_stabilize.c	2017-0381[39]
9.3	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	FrameworkListener.cpp	2016-3921[54]
9.3	-بدست‌آوردن حقوق مازاد، از	متوسط	کامل	کامل	camera_metadata.c	2016-3916[55]

	طریق برنامه کاربردی مخدوش					
9.3	-بستن سوکت به شکل نادرست -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	Java Debug Wire Protocol (JDWP) در adb/sockets.cpp	2016-3890[59]
9.3	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	codecs/on2/dec/SoftVPX.cpp	2016-3872[63]
9.3	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	سریز بافر در codecs/mp3dec/SoftMP3.cpp	2016-3871[64]
9.3	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	SimpleSoftOMXComponent.cpp	2016-3870[65]
9.3	-استفاده نادرست از تبدیلات مابین کدگذاری کاراکتری Unicode و سایر کدگذاری‌ها -اجرای کد دلخواه -سبب منع‌سرویس -سریز بافر مبتنی بر هیپ	متوسط	کامل	کامل	LibUtils	2016-3861[66]
10	-شناسایی نادرست استفاده‌های مجدد[61] از نشست[62] -اجرای کد دلخواه	کم	کامل	کامل	Conscrypt	2016-3840[67]
10	-بدست‌آوردن حقوق، از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	Use-after-free در جزء mm-video-v4l2 venc	2016-3747[75]
9.3	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	متوسط	کامل	کامل	سرریز عدد صحیح در h264bsd_storage.c/	2016-2507[77]
10	-عدم اعتبارسنجی آفست معین -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	کم	کامل	کامل	DRMExtractor.cpp از libstagefright	2016-2506[78]
9.3	- اجرای کد دلخواه یا سبب منع‌سرویس از طریق فایل mkv مخدوش	متوسط	کامل	کامل	libvpx از libwebm	2016-2464[82]
9.3	-عدم اعتبارسنجی اندازه بافر -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	SoftAMR.cpp	2016-2452[86]
9.3	-عدم اعتبارسنجی شناسه‌های قالب[63] -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	Camera3Device.cpp/	2016-2449[87]
9.3	-استفاده نادرست از ارجاعات	متوسط	کامل	کامل	libs/binder/IPCThreadState.cpp	2016-2440[88]

[61] Reuse
[62] Session
[63] Template IDs

	شیء -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش					
9.3	-بدست‌آوردن حقوق از طریق یک برنامه کاربردی شامل نام سمبل مخدوش	متوسط	کامل	کامل	libbacktrace/Backtrace.cpp از debuggerd	2016-2430[89]
10	-ممانعت از عملیات آزاد بر روی حافظه بدون مقداردهی اولیه -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه هیپ) از طریق فایل رسانه مخدوش	کم	کامل	کامل	libFLAC/stream_decoder.c	2016-2429[90]
10	-محدودسازی نامناسب تعداد نخها -اجرای کد دلخواه یا یا سبب منع‌سرویس (خرابی حافظه پشته) از طریق فایل رسانه مخدوش	کم	کامل	کامل	libAACdec/src/aacdec_drc.cpp	2016-2428[91]
9.3	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	rootdir/init.rc	2016-2420[94]
10	-عدم مقداردهی اولیه ساختمان داده پارامتر -بدست‌آوردن اطلاعات حساس از حافظه پردازش -ردنمودن مکانیزم حفاظت	کم	کامل	کامل	media/libmedia/IOMX.cpp	2016-2417[95]
10	-عدم بررسی برای مجوز android Permission DUMP -بدست‌آوردن اطلاعات حساس -ردنمودن مکانیزم حفاظت از طریق درخواست dump	کم	کامل	کامل	BufferQueueConsumer.cpp	2016-2416[96]
7.2	-فرض نامناسب در اندازه هیپ -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	libs/binder/IMemory.cpp	2016-0846[102]
7.2	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	Qualcomm ARM processor performance-event manager	2016-0843[103]
9.3	-عدم نیاز به متد ICameraService:dump برای dump سرویس دوربین - بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوشی که	متوسط	کامل	کامل	Libcameraservice	2016-0826[107]

	مستقیماً dump می‌کند					

4-4-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل اندروید 4.2.1 موجود در ایران، تلفن‌های همراه هوشمند و تلویزیون‌های هوشمند می‌باشند. در واقع اندروید به عنوان سیستم‌عاملی رایج بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشند. در این کار تمرکز بر روی تلویزیون‌های هوشمند می‌باشد. در مبحث تلویزیون‌های هوشمند، سیستم‌عامل اندروید در تلویزیون‌های هوشمند شرکت‌های Sony، XVision، Sharp، Toshiba، Snowa استفاده شده است. هریک از شرکت‌های سازنده از نسخه‌های مختلفی از این سیستم‌عامل بهره برده‌اند. مورد استفاده از سیستم‌عامل اندروید 4.2.1 در تلویزیون هوشمند XVision 50XS520S Smart LED TV می‌باشد. تلویزیون هوشمند مذکور متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشد.

4-5- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4

ارزیابی آسیب‌پذیری‌ها موجود در سیستم‌عامل اندروید 4.4 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم عامل در صورتی که محرمانگی بی‌تاثیر باشد، در جدول 8 بیان شده است.

جدول 8- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0603[3]	libstagefright	بی‌تاثیر	کامل	بالا	-منع سرویس -تعلیق[64] /راه‌اندازی مجدد[65] دستگاه	5.4
2017-0491[25]	ترفیع در حقوق در Package Manager	جزئی	بی‌تاثیر	متوسط	- مانع کاربران از پاک‌کردن[66] برنامه‌های کاربردی یا حذف مجوزها از برنامه‌های کاربردی - ردشدن[67] محلی از نیازمندی‌های تعاملی کاربران	4.3
2017-0489[26]	ترفیع در حقوق در Location Manager	جزئی	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS -تولید داده نادرست	4.3
2017-0422[32]	منع‌سرویس در Bionic DNS	بی‌تاثیر	کامل	کم	- استفاده از بسته شبکه مخدوش جهت تعلیق یا راه‌اندازی مجدد دستگاه	7.8
2017-0395[41]	ترفیع در حقوق در Contacts	جزئی	بی‌تاثیر	متوسط	-ساخت اطلاعات مخاطب جدید - دسترسی به عملیاتی که ممکن است بطور معمول نیازمند مقداردهی	4.3

[64] Hang
[65] Reboot
[66] Uninstalling
[67] Bypass

2017-0393[43]	منع‌سرویس در libvpx	بی‌تاثیر	کامل	جزئی	اولیه یا اجازه کاربر باشد	7.1
2017-0390[44]	منع‌سرویس در Tremolo/dpen.s	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6766[47]	منع‌سرویس در libmedia	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6763[48]	منع‌سرویس در Telephony	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-5348[53]	منع سرویس با استفاده از GPS توسط مهاجمین مردمیانی[۶۸]	بی‌تاثیر	کامل	متوسط	- مصرف حافظه و تعلیق یا راه اندازی مجدد دستگاه از طریق فایل xtra.bin یا xtra2.bin روی یک میزبان	7.1
2016-3881[61]	تابع decoder_peek_si_internal در vp9/vp9_dx_iface.c	بی‌تاثیر	کامل	متوسط	-منع‌سرویس (خواندن بیش از اندازه[۶۹]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3879[62]	arm-wt-22k/lib_src/eas_mdls.c	بی‌تاثیر	کامل	متوسط	- سبب منع‌سرویس (ارجاع اشاره‌گر تهی[۷۰]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3831[72]	منع سرویس با جز telephony	بی‌تاثیر	جزئی	کم	-کاربرد نادرست توسط ساعت سیستم و منع سرویس (خرابی دستگاه) از طریق مقدار زمانی NITZ 2038-01-19 یا بعدتر	5
2016-2495[81]	SampleTable.cpp	بی‌تاثیر	کامل	متوسط	- منع‌سرویس (تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل مخدوش	7.1
2016-2424[93]	SyncStorageEngine.java از SyncStorageEngine	بی‌تاثیر	کامل	متوسط	-مدیریت نادرست داده مرجع معین - منع‌سرویس (حلقه راه‌اندازی مجدد) از طریق برنامه کاربردی مخدوش	7.1
2016-0818[108]	کش‌سازی در کلاس TrustManagerImpl از TrustManagerImpl.java	جزئی	بی‌تاثیر	متوسط	-کاربرد نادرست تمایز مابین CA میانی و CA ریشه مطمئن - مهاجمین مرد میانی می‌توانند سرورها را بوسیله پوشش دسترسی به CA میانی، جعل نمایند	4.3

[68] Man in the middle attackers
[69] Buffer over-read
[70] Null Pointer Reference

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4 با محرمانگی جزئی در جدول 9 بیان شده است.

جدول 9- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4 با محرمانگی جزئی

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0602[4]	افشاء اطلاعات در بلوتوث	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS	4.3
2017-0598[5]	افشای اطلاعات در قالب‌کاری API	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS -بدست‌آوردن حق دسترسی به داده بدون مجوز	4.3
2017-0560[11]	افشای اطلاعات در پردازش بازگشت به تنظیمات کارخانه	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده صاحب قبلی -احتمال ردشدن از حفاظت دستگاه	4.3
2017-0559[12]	افشای اطلاعات در libskia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0558[13]	افشای اطلاعات در Mediaserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0554[14]	ترفیع در حقوق در جزء تلفن	جزئی	جزئی	متوسط	-بدست‌آوردن توانایی‌های ترفیع یافته	6.8
2017-0547[16]	افشای اطلاعات در libmedia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز -ردشدن عمومی از حفاظت‌های OS	4.3
2017-0425[31]	افشای اطلاعات در Audioserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0420[34]	افشای اطلاعات در AOSP Mail	بی‌تاثیر	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS (OS مسئول جداسازی برنامه کاربردی از سایر برنامه‌های کاربردی می‌باشد)	4.3
2017-0402[37]	افشای اطلاعات در EffectBundle.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0401[38]	افشای اطلاعات در EffectBundle.cpp از Qualcomm audio	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0396[40]	افشای اطلاعات در EffectVisualizer.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2016-6703[51]	اجرای کد راه دور در یک کتابخانه زمان اجرای اندروید	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-6702[52]	اجرای کد راه دور در libjpeg	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-3897[57]	کلاس WifiEnterpriseConfig در WifiEnterpriseConfig.java	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش و رمز عبور موجود در مقدار بازگشتی از متد فراخوانی (به صورت رشته از این کلاس)	4.3
2016-3896[58]	AOSP Mail و اطلاعات EmailAccountCacheProvider	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست‌آوردن اطلاعات از طریق برنامه کاربردی مخدوش	4.3
2016-3835[70]	نشست امن در جزء mm-video-v4l2 venc	بی‌تاثیر	بی‌تاثیر	متوسط	-استفاده نادرست از اشاره‌گرهای هیپ -بدست‌آوردن اطلاعات حساس از	4.3

	طریق برنامه کاربردی مخدوش					
2016-3834[71]	camera APIs	بی‌تاثیر	بی‌تاثیر	متوسط	-رد نمودن محدودیت دسترسی -بدست‌آوردن اطلاعات حساس درباره آدرس‌های بافر ANW از طریق برنامه کاربردی مخدوش	4.3
2016-3822[73]	exif.c استفاده‌شده در libjhead	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (دسترسی خارج از محدوده) از طریق داده EXIF مخدوش	7.5
2016-3761[74]	NfcService.java در NFC	بی‌تاثیر	بی‌تاثیر	کم	-بدست‌آوردن اطلاعات برنامه کاربردی پیش‌زمینه[71] حساس از طریق برنامه کاربردی پس‌زمینه مخدوش	2.1
2016-3744[76]	سرریز بافر در create_pbuf function در btif/src/btif_hh.c در بلوتوث	جزئی	جزئی	بالا	-بدست‌آوردن حقوق از طریق عملیات جفت‌سازی مخدوش	4.3
2016-2499[80]	AudioSource.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-مقداردهی اولیه نادرست -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-2463[83]	سرریز عدد صحیح در جزء h264dec	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	7.5
2016-2426[92]	جزء قالب‌کاری ContentService.java	بی‌تاثیر	بی‌تاثیر	متوسط	-عدم بررسی جهت مجوز GET_ACCOUNTS -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-1155[99]	تزریق سرآیند Http در کلاس URLConnection	جزئی	جزئی	کم	-اجرای اسکریپت‌های دلخواه یا مقداردهی مقادیر دلخواه را در کوکی‌ها[72]	7.5
2016-0850[100]	PORCHE_PAIRING_CONFLIC در بلوتوث	جزئی	جزئی	کم	-ردنمودن محدودیت‌های جفت‌سازی از طریق دستگاه مخدوش	5.8
2016-0829[105]	BnGraphicBufferProducer.onTra در IGraphicBufferConsumer.cpp	بی‌تاثیر	بی‌تاثیر	کم	-عدم مقداردهی اولیه برای ساختارداده‌ای معین -بدست‌آوردن اطلاعات حساس -ردنمودن حفاظت بوسیله راه‌اندازی فعالیت QUEUE_BUFFER	5

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4 با محرمانگی کامل در جدول 10 بیان شده است.

[71] Foreground
[72] Cookies

جدول 10- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4 با محرمانگی کامل

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0596[6]	ترفیع در حقوق libstagefright	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0594[7]	ترفیع در حقوق SoftAACEncoder2.cpp	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0592[8]	اجرای کد راه دور FLACExtractor.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0588[10]	اجرای کد راه دور درid3/ID3.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0546[17]	ترفیع در حقوق در SurfaceFlinger	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0544[19]	ترفیع در حقوق در CameraBase	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3
2017-0541[20]	اجرای کد راه دور در sonivox	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده - احتمال اجرای کد راه دور در داخل مفهوم پردازش Mediaserver	9.3
2017-0480[28]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن توانایی‌های ترفیع‌یافته	9.3
2017-0475[30]	ترفیع در حقوق در recovery verifier	کامل	کامل	متوسط	-اجرای کد دلخواه در هسته -حیاتی بدلیل احتمال مخرب بودن دائمی دستگاه محلی - سبب پاک‌سازی و قرارگیری مجدد سیستم عامل برای ترمیم دستگاه	9.3
2017-0419[35]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	9.3
2017-0381[39]	افشای اطلاعات در silk/NLSF_stabilize.c	کامل	کامل	متوسط	-دسترسی به داده حساس بدون مجوز	9.3
2016-3921[54]	FrameworkListener.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از	9.3

					طریق برنامه کاربردی مخدوش	
2016-3916[55]	camera_metadata.c	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3890[59]	Java Debug Wire Protocol (JDWP) در adb/sockets.cpp	کامل	کامل	متوسط	-بستن سوکت به شکل نادرست -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	9.3
2016-3872[63]	codecs/on2/dec/SoftVPX.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3871[64]	سریز بافر در codecs/mp3dec/SoftMP3.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3870[65]	SimpleSoftOMXComponent.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3861[66]	LibUtils	کامل	کامل	متوسط	-استفاده نادرست از تبدیلات مابین کدگذاری کاراکتری Unicode و سایر کدگذاری‌ها -اجرای کد دلخواه -سبب منع‌سرویس -سریز بافر مبتنی بر هیپ	9.3
2016-3840[67]	Conscrypt	کامل	کامل	کم	-شناسایی نادرست استفاده‌های مجدد[۷۳] از نشست[74] -اجرای کد دلخواه	10
2016-3747[75]	Use-after-free در جزء mm-video-v4l2 venc	کامل	کامل	کم	-بدست‌آوردن حقوق، از طریق برنامه کاربردی مخدوش	10
2016-2507[77]	سریز عدد صحیح در h264bsd_storage.c/	کامل	کامل	متوسط	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	9.3
2016-2506[78]	DRMExtractor.cpp از libstagefright	کامل	کامل	کم	-عدم اعتبارسنجی آفست معین -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	10
2016-2452[86]	SoftAMR.cpp	کامل	کامل	متوسط	-عدم اعتبارسنجی اندازه بافر -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	9.3
2016-2449[87]	Camera3Device.cpp/	کامل	کامل	متوسط	-عدم اعتبارسنجی شناسه‌های قالب[۷۵] -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	9.3
2016-2440[88]	libs/binder/IPCThreadState.cpp	کامل	کامل	متوسط	-استفاده نادرست از ارجاعات شیء	9.3

[73] Reuse
[74] Session
[75] Template IDs

	-بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش					
9.3	-بدست‌آوردن حقوق از طریق یک برنامه کاربردی شامل نام سمبل مخدوش	متوسط	کامل	کامل	libbacktrace/Backtrace.cpp از debuggerd	2016-2430[89]
10	-ممانعت از عملیات آزاد بر روی حافظه بدون مقداردهی اولیه -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه هیپ) از طریق فایل رسانه مخدوش	کم	کامل	کامل	libFLAC/stream_decoder.c	2016-2429[90]
10	-محدودسازی نامناسب تعداد نخ‌ها -اجرای کد دلخواه یا یا سبب منع‌سرویس (خرابی حافظه پشته) از طریق فایل رسانه مخدوش	کم	کامل	کامل	libAACdec/src/aacdec_drc.cpp	2016-2428[91]
9.3	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	rootdir/init.rc	2016-2420[94]
10	-عدم مقداردهی اولیه ساختمان داده پارامتر -بدست‌آوردن اطلاعات حساس از حافظه پردازش -ردنمودن مکانیزم حفاظت	کم	کامل	کامل	media/libmedia/IOMX.cpp	2016-2417[95]
10	-عدم بررسی برای مجوز android permission DUMP -بدست‌آوردن اطلاعات حساس -ردنمودن مکانیزم حفاظت از طریق درخواست dump	کم	کامل	کامل	BufferQueueConsumer.cpp	2016-2416[96]
7.2	-فرض نامناسب در اندازه هیپ -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	libs/binder/IMemory.cpp	2016-0846[102]
7.2	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	Qualcomm ARM processor performance-event manager	2016-0843[103]
9.3	-عدم نیاز به متد ICameraService:dump برای dump سرویس دوربین - بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوشی که مستقیماً dump می‌کند	متوسط	کامل	کامل	Libcameraservice	2016-0826[107]

3-10-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل اندروید 4.4 موجود در ایران، تلفن‌های همراه هوشمند و تلویزیون‌های هوشمند می‌باشند. در واقع اندروید به عنوان سیستم‌عاملی رایج بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشند. در این کار تمرکز بر روی تلویزیون‌های هوشمند می‌باشد. مورد استفاده از سیستم‌عامل اندروید 4.4 در تلویزیون هوشمند موجود در ایران، TOSHIBA LED Smart TV 47L5450 می‌باشد که تلویزیون هوشمند مذکور متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشد.

3-11- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.2

ارزیابی آسیب‌پذیری‌ها موجود در سیستم‌عامل اندروید 4.4.2 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم‌عامل در صورتی که محرمانگی بی‌تاثیر باشد، در جدول 11 بیان شده است.

جدول 11 - آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.2 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0603[3]	libstagefright	بی‌تاثیر	کامل	بالا	-منع سرویس -تعلیق[۷۶] /راه‌اندازی مجدد[۷۷] دستگاه	5.4
2017-0491[25]	ترفیع در حقوق در Package Manager	جزئی	بی‌تاثیر	متوسط	- مانع کاربران از پاک‌کردن[۷۸] برنامه‌های کاربردی یا حذف مجوزها از برنامه‌های کاربردی - ردشدن[۷۹] محلی از نیازمندی‌های تعاملی کاربران	4.3
2017-0489[26]	ترفیع در حقوق در Location Manager	جزئی	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS -تولید داده نادرست	4.3
2017-0422[32]	منع‌سرویس در Bionic DNS	بی‌تاثیر	کامل	کم	- استفاده از بسته شبکه مخدوش جهت تعلیق یا راه‌اندازی مجدد دستگاه	7.8
2017-0395[41]	ترفیع در حقوق در Contacts	جزئی	بی‌تاثیر	متوسط	-ساخت اطلاعات مخاطب جدید - دسترسی به عملیاتی که ممکن است بطور معمول نیازمند مقداردهی اولیه یا اجازه کاربر باشد	4.3
2017-0393[43]	منع‌سرویس در libvpx	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2017-0390[44]	منع‌سرویس در Tremolo/dpen.s	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد	7.1

[76] Hang
[77] Reboot
[78] Uninstalling
[79] Bypass

2016-6766[47]	منع‌سرویس در libmedia	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6763[48]	منع‌سرویس در Telephony	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-5348[53]	منع سرویس با استفاده از GPS توسط مهاجمین مردمیانی[80]	بی‌تاثیر	کامل	متوسط	- مصرف حافظه و تعلیق یا راه اندازی مجدد دستگاه از طریق فایل xtra.bin یا xtra2.bin روی یک میزبان	7.1
2016-3881[61]	تابع decoder_peek_si_internal در vp9/vp9_dx_iface.c	بی‌تاثیر	کامل	متوسط	-منع‌سرویس (خواندن بیش از اندازه[81]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3879[62]	arm-wt-22k/lib_src/eas_mdls.c	بی‌تاثیر	کامل	متوسط	- سبب منع‌سرویس (ارجاع اشاره‌گر تهی[82]، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-2495[81]	SampleTable.cpp	بی‌تاثیر	کامل	متوسط	- منع‌سرویس (تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل مخدوش	7.1
2016-2424[93]	SyncStorageEngine.java از SyncStorageEngine	بی‌تاثیر	کامل	متوسط	-مدیریت نادرست داده مرجع معین - منع‌سرویس (حلقه راه‌اندازی مجدد) از طریق برنامه کاربردی مخدوش	7.1
2016-0818[108]	کش‌سازی در کلاس TrustManagerImpl از TrustManagerImpl.java	جزئی	بی‌تاثیر	متوسط	-کاربرد نادرست تمایز مابین CA میانی و CA ریشه مطمئن - مهاجمین مرد میانی می‌توانند سرورها را بوسیله پوشش دسترسی به CA میانی، جعل نمایند	4.3

آسیب‌پذیری موجود در سیستم‌عامل اندروید 4.4.2 با محرمانگی جزئی در جدول 12 بیان شده است.

جدول 12- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.2 با محرمانگی جزئی

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0602[4]	افشاء اطلاعات در بلوتوث	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS	4.3
2017-0598[5]	افشای اطلاعات در قالب‌کاری API	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS	4.3

[80] Man in the middle attackers
[81] Buffer over-read
[82] Null Pointer Reference

					-بدست‌آوردن حق دسترسی به داده بدون مجوز	
2017-0560[11]	افشای اطلاعات در پردازش بازگشت به تنظیمات کارخانه	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده صاحب قبلی -احتمال ردشدن از حفاظت دستگاه	4.3
2017-0559[12]	افشای اطلاعات در libskia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0558[13]	افشای اطلاعات در Mediaserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0554[14]	ترفیع در حقوق در جزء تلفن	جزئی	جزئی	متوسط	-بدست‌آوردن توانایی‌های ترفیع یافته	6.8
2017-0547[16]	افشای اطلاعات در libmedia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز -ردشدن عمومی از حفاظت‌های OS	4.3
2017-0425[31]	افشای اطلاعات در Audioserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0420[34]	افشای اطلاعات در AOSP Mail	بی‌تاثیر	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS (OS مسئول جداسازی برنامه کاربردی از سایر برنامه‌های کاربردی می‌باشد)	4.3
2017-0402[37]	افشای اطلاعات در EffectBundle.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0401[38]	افشای اطلاعات در EffectBundle.cpp از Qualcomm audio	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0396[40]	افشای اطلاعات در EffectVisualizer.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2016-6703[51]	اجرای کد راه دور در یک کتابخانه زمان اجرای اندروید	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-6702[52]	اجرای کد راه دور در libjpeg	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-3897[57]	کلاس WifiEnterpriseConfig در WifiEnterpriseConfig.java	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش و رمز عبور موجود در مقدار بازگشتی از متد فراخوانی (به صورت رشته از این کلاس)	4.3
2016-3896[58]	AOSP Mail و اطلاعات EmailAccountCacheProvider	بی‌تاثیر	بی‌تاثیر	متوسط	-بدست‌آوردن اطلاعات از طریق برنامه کاربردی مخدوش	4.3
2016-3835[70]	نشست امن در جزء mm-video-v4l2 venc	بی‌تاثیر	بی‌تاثیر	متوسط	-استفاده نادرست از اشاره‌گرهای هیپ -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-3834[71]	camera APIs	بی‌تاثیر	بی‌تاثیر	متوسط	-رد نمودن محدودیت دسترسی -بدست‌آوردن اطلاعات حساس درباره آدرس‌های بافر ANW از طریق برنامه کاربردی مخدوش	4.3
2016-3822[73]	exif.c استفاده‌شده در libjhead	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (دسترسی خارج از محدوده) از طریق داده EXIF	7.5

2016-3761[74]	NfcService.java در NFC	بی‌تاثیر	بی‌تاثیر	کم	-بدست‌آوردن اطلاعات برنامه کاربردی پیش‌زمینه[۸۳] حساس از طریق برنامه کاربردی پس‌زمینه مخدوش	2.1
2016-3744[76]	سرریز بافر در create_pbuf function در btif/src/btif_hh.c در بلوتوث	جزئی	جزئی	بالا	-بدست‌آوردن حقوق از طریق عملیات جفت‌سازی مخدوش	4.3
2016-2499[80]	AudioSource.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-مقداردهی اولیه نادرست -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-2463[83]	سرریز عدد صحیح در جزء h264dec	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	7.5
2016-2426[92]	جزء قالب‌کاری ContentService.java	بی‌تاثیر	بی‌تاثیر	متوسط	-عدم بررسی جهت مجوز GET_ACCOUNTS -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-1155[99]	تزریق سرآیند Http در کلاس URLConnection	جزئی	جزئی	کم	-اجرای اسکریپت‌های دلخواه یا مقداردهی مقادیر دلخواه را در کوکی‌ها[۸۴]	7.5
2016-0850[100]	PORCHE_PAIRING_CONFLIC در بلوتوث	جزئی	جزئی	کم	-ردنمودن محدودیت‌های جفت‌سازی از طریق دستگاه مخدوش	5.8
2016-0829[105]	BnGraphicBufferProducer.onTra در IGraphicBufferConsumer.cpp	بی‌تاثیر	بی‌تاثیر	کم	-عدم مقداردهی اولیه برای ساختارداده‌ای معین -بدست‌آوردن اطلاعات حساس -ردنمودن حفاظت بوسیله راه‌اندازی فعالیت QUEUE_BUFFER	5

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.2 با محرمانگی کامل در جدول 13 بیان شده است.

جدول 13 - آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.2 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0596[6]	ترفیع در حقوق libstagefright	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0594[7]	ترفیع در حقوق SoftAACEncoder2.cpp	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم	9.3

[83] Foreground
[84] Cookies

					پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	
2017-0592[8]	اجرای کد راه دور FLACExtractor.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0588[10]	اجرای کد راه دور درid3/ID3.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0546[17]	ترفیع در حقوق در SurfaceFlinger	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0544[19]	ترفیع در حقوق در CameraBase	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3
2017-0541[20]	اجرای کد راه دور در sonivox	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده - احتمال اجرای کد راه دور در داخل مفهوم پردازش Mediaserver	9.3
2017-0480[28]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن تونایی‌های ترفیع‌یافته	9.3
2017-0475[30]	ترفیع در حقوق در recovery verifier	کامل	کامل	متوسط	-اجرای کد دلخواه در هسته -حیاتی بدلیل احتمال مخرب بودن دائمی دستگاه محلی - سبب پاک‌سازی و قرارگیری مجدد سیستم عامل برای ترمیم دستگاه	9.3
2017-0419[35]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	9.3
2017-0381[39]	افشای اطلاعات در silk/NLSF_stabilize.c	کامل	کامل	متوسط	-دسترسی به داده حساس بدون مجوز	9.3
2016-3921[54]	FrameworkListener.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3916[55]	camera_metadata.c	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3890[59]	Java Debug Wire Protocol (JDWP) در adb/sockets.cpp	کامل	کامل	متوسط	-بستن سوکت به شکل نادرست -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	9.3
2016-3872[63]	codecs/on2/dec/SoftVPX.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3

2016-3871[64]	سریز بافر در codecs/mp3dec/SoftMP3.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3870[65]	SimpleSoftOMXComponent.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3861[66]	LibUtils	کامل	کامل	متوسط	-استفاده نادرست از تبدیلات مابین کدگذاری کاراکتری Unicode و سایر کدگذاری‌ها -اجرای کد دلخواه -سبب منع‌سرویس -سریز بافر مبتنی بر هیپ	9.3
2016-3840[67]	Conscrypt	کامل	کامل	کم	-شناسایی نادرست استفاده‌های مجدد[85] از نشست[86] -اجرای کد دلخواه	10
2016-3747[75]	Use-after-free در جزء mm-video-v4l2 venc	کامل	کامل	کم	-بدست‌آوردن حقوق، از طریق برنامه کاربردی مخدوش	10
2016-2507[77]	سرریز عدد صحیح در /h264bsd_storage.c	کامل	کامل	متوسط	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	9.3
2016-2506[78]	DRMExtractor.cpp از libstagefright	کامل	کامل	کم	-عدم اعتبارسنجی آفست معین -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	10
2016-2452[86]	SoftAMR.cpp	کامل	کامل	متوسط	-عدم اعتبارسنجی اندازه بافر -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	9.3
2016-2449[87]	Camera3Device.cpp/	کامل	کامل	متوسط	-عدم اعتبارسنجی شناسه‌های قالب[87] -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	9.3
2016-2440[88]	libs/binder/IPCThreadState.cpp	کامل	کامل	متوسط	-استفاده نادرست از ارجاعات شیء -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	9.3
2016-2430[89]	libbacktrace/Backtrace.cpp از debuggerd	کامل	کامل	متوسط	-بدست‌آوردن حقوق از طریق یک برنامه کاربردی شامل نام سمبل مخدوش	9.3
2016-2429[90]	libFLAC/stream_decoder.c	کامل	کامل	کم	-ممانعت از عملیات آزاد بر روی حافظه بدون مقداردهی اولیه -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه هیپ)	10

[85] Reuse
[86] Session
[87] Template IDs

	از طریق فایل رسانه مخدوش					
10	-محدودسازی نامناسب تعداد نخ‌ها -اجرای کد دلخواه یا یا سبب منع‌سرویس (خرابی حافظه پشته) از طریق فایل رسانه مخدوش	کم	کامل	کامل	libAACdec/src/aacdec_drc.cpp	2016-2428[91]
9.3	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	rootdir/init.rc	2016-2420[94]
10	-عدم مقداردهی اولیه ساختمان داده پارامتر -بدست‌آوردن اطلاعات حساس از حافظه پردازش -ردنمودن مکانیزم حفاظت	کم	کامل	کامل	media/libmedia/IOMX.cpp	2016-2417[95]
10	-عدم بررسی برای مجوز android permission DUMP -بدست‌آوردن اطلاعات حساس -ردنمودن مکانیزم حفاظت از طریق درخواست dump	کم	کامل	کامل	BufferQueueConsumer.cpp	2016-2416[96]
7.2	-فرض نامناسب در اندازه هیپ -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	libs/binder/IMemory.cpp	2016-0846[102]
7.2	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	Qualcomm ARM processor performance-event manager	2016-0843[103]
9.3	-عدم نیاز به متد ICameraService:dump برای dump سرویس دوربین - بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوشی که مستقیماً dump می‌کند	متوسط	کامل	کامل	Libcameraservice	2016-0826[107]

3-11-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل اندروید 4.4.2 موجود در ایران، تلفن‌های همراه هوشمند و تلویزیون‌های هوشمند می‌باشند. در واقع اندروید به عنوان سیستم‌عاملی رایج بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشند. در این کار تمرکز بر روی تلویزیون‌های هوشمند می‌باشد. مورد استفاده از سیستم‌عامل اندروید 4.4.2 در تلویزیون‌های هوشمند موجود در ایران مربوط به برخی محصولات شرکت TOSHIBA می‌باشند. تلویزیون‌های هوشمند TOSHIBA Full HD 40L5550، TOSHIBA Full HD LED TV 55L5550، TOSHIBA Smart TV LED Full HD 50L5550، TOSHIBA LED Full HD 40L5450، TOSHIBA LED TV Full HD

55L5450 که از اندروید 4.4.2 به عنوان سیستم‌عامل بهره می‌برند، متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشند.

3-12- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4

ارزیابی آسیب‌پذیری‌ها موجود در سیستم‌عامل اندروید 4.4.4 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم عامل در صورتی که محرمانگی بی‌تاثیر باشد، در جدول 14 بیان شده است.

جدول 14- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0603[3]	Libstagefright	بی‌تاثیر	کامل	بالا	-منع سرویس -تعلیق[88] /راه‌اندازی مجدد[89] دستگاه	5.4
2017-0491[25]	ترفیع در حقوق در Package Manager	جزئی	بی‌تاثیر	متوسط	- مانع کاربران از پاک‌کردن[90] برنامه‌های کاربردی یا حذف مجوزها از برنامه‌های کاربردی - ردشدن[91] محلی از نیازمندی‌های تعاملی کاربران	4.3
2017-0489[26]	ترفیع در حقوق در Location Manager	جزئی	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS -تولید داده نادرست	4.3
2017-0422[32]	منع‌سرویس در Bionic DNS	بی‌تاثیر	کامل	کم	- استفاده از بسته شبکه مخدوش جهت تعلیق یا راه‌اندازی مجدد دستگاه	7.8
2017-0395[41]	ترفیع در حقوق در Contacts	جزئی	بی‌تاثیر	متوسط	-ساخت اطلاعات مخاطب جدید - دسترسی به عملیاتی که ممکن است بطور معمول نیازمند مقداردهی اولیه یا اجازه کاربر باشد	4.3
2017-0393[43]	منع‌سرویس در libvpx	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2017-0390[44]	منع‌سرویس در Tremolo/dpen.s	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6766[47]	منع‌سرویس در libmedia	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6763[48]	منع‌سرویس در Telephony	بی‌تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2015-6645[114]	SyncManager	بی‌تاثیر	کامل	متوسط	- سبب منع‌سرویس (راه‌اندازی مجدد بطور مداوم) از طریق برنامه کاربردی مخدوش	7.1

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4 با محرمانگی جزئی در جدول 15 بیان شده است.

[88] Hang
[89] Reboot
[90] Uninstalling
[91] Bypass

جدول 15- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4 با محرمانگی جزئی

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0602[4]	افشاء اطلاعات در بلوتوث	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS	4.3
2017-0598[5]	افشای اطلاعات در قالب‌کاری API	بی‌تاثیر	بی‌تاثیر	متوسط	-دور زدن حفاظت OS -بدست‌آوردن حق دسترسی به داده بدون مجوز	4.3
2017-0560[11]	افشای اطلاعات در پردازش بازگشت به تنظیمات کارخانه	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده صاحب قبلی -احتمال ردشدن از حفاظت دستگاه	4.3
2017-0559[12]	افشای اطلاعات در libskia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0558[13]	افشای اطلاعات در Mediaserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0554[14]	ترفیع در حقوق در جزء تلفن	جزئی	جزئی	متوسط	-بدست‌آوردن توانایی‌های ترفیع یافته	6.8
2017-0547[16]	افشای اطلاعات در libmedia	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز -ردشدن عمومی از حفاظت‌های OS	4.3
2017-0425[31]	افشای اطلاعات در Audioserver	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0420[34]	افشای اطلاعات در AOSP Mail	بی‌تاثیر	بی‌تاثیر	متوسط	-ردنمودن حفاظت‌های OS (OS مسئول جداسازی برنامه کاربردی از سایر برنامه‌های کاربردی می‌باشد)	4.3
2017-0402[37]	افشای اطلاعات در EffectBundle.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0401[38]	افشای اطلاعات در EffectBundle.cpp از Qualcomm audio	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0396[40]	افشای اطلاعات در EffectVisualizer.cpp	بی‌تاثیر	بی‌تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2016-6703[51]	اجرای کد راه دور در یک کتابخانه زمان اجرای اندروید	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-1155[99]	تزریق سرآیند Http در کلاس URLConnection	جزئی	جزئی	کم	-اجرای اسکریپت‌های دلخواه یا مقداردهی مقادیر دلخواه را در کوکی‌ها[92]	7.5

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4 با محرمانگی کامل در جدول 16 بیان شده است.

جدول 16- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 4.4.4 با محرمانگی کامل

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0596[6]	ترفیع در حقوق libstagefright	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3

[92] Cookies

	-بدست‌آوردن توانایی ترفیع‌یافته					
2017-0594[7]	ترفیع در حقوق SoftAACEncoder2.cpp	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0592[8]	اجرای کد راه دور FLACExtractor.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0588[10]	اجرای کد راه دور درid3/ID3.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0546[17]	ترفیع در حقوق در SurfaceFlinger	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0544[19]	ترفیع در حقوق در CameraBase	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3
2017-0541[20]	اجرای کد راه دور در sonivox	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده - احتمال اجرای کد راه دور در داخل مفهوم پردازش Mediaserver	9.3
2017-0480[28]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن تونایی‌های ترفیع‌یافته	9.3
2017-0475[30]	ترفیع در حقوق در recovery verifier	کامل	کامل	متوسط	-اجرای کد دلخواه در هسته -حیاتی بدلیل احتمال مخرب بودن دائمی دستگاه محلی - سبب پاک‌سازی و قرارگیری مجدد سیستم عامل برای ترمیم دستگاه	9.3
2017-0419[35]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	9.3
2017-0381[39]	افشای اطلاعات در silk/NLSF_stabilize.c	کامل	کامل	متوسط	-دسترسی به داده حساس بدون مجوز	9.3
2016-0802[113]	Broadcom Wi-Fi driver	کامل	کامل	کم	-اجرای کد دلخواه یا سبب منع سرویس (خرابی حافظه) از طریق بسته‌های پیام کنترلی بی سیم مخدوش	8.3

3-12-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل اندروید 4.4.4 موجود در ایران، تلفن‌های همراه هوشمند و تلویزیون‌های هوشمند می‌باشند. در واقع اندروید به عنوان سیستم‌عاملی رایج بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشند. در این کار تمرکز بر روی تلویزیون‌های هوشمند می‌باشد. مورد استفاده از سیستم‌عامل

اندروید 4.4.4 در تلویزیون‌های هوشمند موجود در ایران مربوط به برخی محصولات شرکت XVision می‌باشد. تلویزیون هوشمند XVision 55XK530S Smart LED TV که از اندروید 4.4.4 به عنوان سیستم‌عامل بهره می‌برد، متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشد.

13-3- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1

ارزیابی آسیب‌پذیری‌ها موجود در سیستم‌عامل اندروید 5.1 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم عامل در صورتی که محرمانگی بی‌تاثیر باشد، در جدول 17 بیان شده است.

جدول 17- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1 با محرمانگی بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0603[3]	libstagefright	بی تاثیر	کامل	بالا	-منع سرویس -تعلیق۹۳ /راه‌اندازی مجدد۹۴ دستگاه	5.4
2017-0499[22]	منع‌سرویس در Audioserver	بی تاثیر	کامل	متوسط	- باعث تعلیق یا راه‌اندازی مجدد دستگاه	7.1
2017-0498[23]	منع‌سرویس در Setup Wizard	بی تاثیر	جزئی	کم	- دستیابی به اطلاعات کاربر توسط مهاجم محلی (یعنی ورود به حساب کاربری گوگل بعد از بازگشت به تنظیمات کارخانه برای کاربر، ضروری باشد)	2.1
2017-0496[24]	منع‌سرویس در Setup Wizard	بی تاثیر	جزئی	متوسط	-بلوکه نمودن موقت دسترسی به دستگاه آلوده‌شده توسط برنامه کاربردی مخرب محلی -نیازمند بازگشت به تنظیمات کارخانه برای ترمیم دستگاه	4.3
2017-0491[25]	ترفیع در حقوق در Package Manager	جزئی	بی تاثیر	متوسط	- مانع کاربران از پاک‌کردن۹۵ برنامه‌های کاربردی یا حذف مجوزها از برنامه‌های کاربردی - ردشدن۹۶ محلی از نیازمندی‌های تعاملی کاربران	4.3
2017-0489[26]	ترفیع در حقوق در Location Manager	جزئی	بی تاثیر	متوسط	-ردنمودن حفاظت‌های OS -تولید داده نادرست	4.3
2017-0483[27]	منع‌سرویس در Mediaserver	بی تاثیر	کامل	متوسط	- سبب تعلیق یا راه‌اندازی مجدد دستگاه توسط فایل مخدوش	7.1
2017-0422[32]	منع‌سرویس	بی	کامل	کم	- استفاده از بسته شبکه مخدوش جهت	7.8

[93] Hang
[94] Reboot
[95] Uninstalling
[96] Bypass

	در Bionic DNS	تاثیر			تعلیق یا راه‌اندازی مجدد دستگاه	
2017-0395[41]	ترفیع در حقوق در Contacts	جزئی	بی تاثیر	متوسط	-ساخت اطلاعات مخاطب جدید - دسترسی به عملیاتی که ممکن است بطور معمول نیازمند مقداردهی اولیه یا اجازه کاربر باشد	4.3
2017-0394[42]	منع‌سرویس در Telephony	بی تاثیر	کامل	کم	- باعث تعلیق یا راه‌اندازی مجدد دستگاه	7.8
2017-0393[43]	منع‌سرویس در libvpx	بی تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2017-0390[44]	منع‌سرویس در Tremolo/dpen.s	بی تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6769[46]	ترفیع در حقوق در Smart Lock	جزئی	بی تاثیر	کم	-دسترسی به تنظیمات قفل هوشمند بدون PIN	2.1
2016-6766[47]	منع‌سرویس در libmedia	بی تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-6763[48]	منع‌سرویس در Telephony	بی تاثیر	کامل	متوسط	- سبب تعلیق و راه‌اندازی مجدد دستگاه	7.1
2016-5348[53]	منع سرویس با استفاده از GPS توسط مهاجمین مردمیانی۹۷	بی تاثیر	کامل	متوسط	- مصرف حافظه و تعلیق یا راه اندازی مجدد دستگاه از طریق فایل xtra.bin یاxtra2.bin روی یک میزبان	7.1
2016-3881[61]	تابع decoder_peek_si_internal در vp9_dx_iface.c	بی تاثیر	کامل	متوسط	-منع‌سرویس (خواندن بیش از اندازه۹۸، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3879[62]	eas_mdls.c	بی تاثیر	کامل	متوسط	- سبب منع‌سرویس (ارجاع اشاره‌گر تهی۹۹، تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل رسانه مخدوش	7.1
2016-3831[72]	منع سرویس با جز telephony	بی تاثیر	جزئی	کم	-کاربرد نادرست توسط ساعت سیستم و منع سرویس (خرابی دستگاه) از طریق مقدار زمانی NITZ 2038-01-19 یا بعدتر	5
2016-2495[81]	SampleTable.cpp	بی تاثیر	کامل	متوسط	- منع‌سرویس (تعلیق یا راه‌اندازی مجدد دستگاه) از طریق فایل مخدوش	7.1
2016-2457[85]	UserManagerService.java	جزئی	بی تاثیر	کم	-ردنمودن محدودیت‌های درنظر گرفته‌شده بر روی تغییرات پیکربندی WiFi بوسیله پوشش دسترسی مهمان۱۰۰	2.1
2016-2424[93]	SyncStorageEngine.java	بی	کامل	متوسط	-مدیریت نادرست داده مرجع معین	7.1

[97] Man in the middle attackers
[98] Buffer over-read
[99] Null Pointer Reference
[100] Guest Access

	از SyncStorageEngine	تاثیر			- منع‌سرویس (حلقه راه‌اندازی مجدد) از طریق برنامه کاربردی مخدوش	
2016-2414[98]	کتابخانه Minikin	بی تاثیر	کامل	کم	-سبب منع سرویس (خرابی حافظه و حلقه راه‌اندازی مجدد) از طریق فرض نامناسب مقادیر منفی در داده Font	4.9
2016-0818[108]	کش‌سازی در کلاس TrustManagerImpl از TrustManagerImpl.java	جزئی	بی تاثیر	متوسط	-کاربرد نادرست تمایز مابین CA میانی و CA ریشه مطمئن - مهاجمین مرد میانی می‌توانند سرورها را بوسیله پوشش دسترسی به CA میانی، جعل نمایند	4.3
2016-0813[109]	AlternateRecentsComponent.java	کامل	کامل	کم	-ردنمودن مکانیزم حفاظت Factory Reset Protection و حذف داده	6.6
2016-0812[110]	interceptKeyBeforeDispatching	کامل	کامل	کم	-عدم بررسی مناسب در فعالیت تکمیل نصب در setup wizard -ردنمودن مکانیزم حفاظت Factory Reset Protection و حذف داده	6.6
2016-0808[111]	سرریز عدد صحیح در تابع getCoverageFormat12	بی تاثیر	کامل	کم	-سبب منع سرویس (راه‌اندازی مجدد به صورت مداوم و پشت سرهم) از طریق برنامه کاربردی (راه‌اندازی رویداد بارگذاری فونت TTF مخدوش توسط برنامه کاربردی) -این تابع در CmapCoverage.cpp از کتابخانه Minikin قرار دارد	4.9
2015-6645[114]	SyncManager	بی تاثیر	کامل	متوسط	- سبب منع‌سرویس (راه‌اندازی مجدد بطور مداوم) از طریق برنامه کاربردی مخدوش	7.1

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1 با محرمانگی جزئی در جدول 18 بیان شده است.

جدول 18- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1 با محرمانگی جزئی

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0602[4]	افشاء اطلاعات در بلوتوث	بی تاثیر	بی تاثیر	متوسط	-دور زدن حفاظت OS	4.3
2017-0598[5]	افشای اطلاعات در قالب‌کاری API	بی تاثیر	بی تاثیر	متوسط	-دور زدن حفاظت OS -بدست‌آوردن حق دسترسی به داده بدون مجوز	4.3
2017-0560[11]	افشای اطلاعات در پردازش بازگشت به تنظیمات کارخانه	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده صاحب قبلی -احتمال ردشدن از حفاظت دستگاه	4.3

2017-0559[12]	افشای اطلاعات در libskia	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0558[13]	افشای اطلاعات در Mediaserver	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0554[14]	ترفیع در حقوق در جزء تلفن	جزئی	جزئی	متوسط	-بدست‌آوردن توانایی‌های ترفیع یافته	6.8
2017-0547[16]	افشای اطلاعات در libmedia	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده بدون مجوز -ردشدن عمومی از حفاظت‌های OS	4.3
2017-0478[29]	اجرای کد راه دور در کتابخانه Framesequence	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -احتمال اجرای کد راه دور در یک برنامه کاربردی	6.8
2017-0425[31]	افشای اطلاعات در Audioserver	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0421[33]	افشای اطلاعات در قالب‌کاری API	بی تاثیر	بی تاثیر	متوسط	-ردنمودن حفاظت OS (OS مسئولیت جداسازی برنامه کاربردی را از دیگر برنامه های کاربردی بر عهده دارد)	4.3
2017-0420[34]	افشای اطلاعات در AOSP Mail	بی تاثیر	بی تاثیر	متوسط	-ردنمودن حفاظت‌های OS (OS مسئول جداسازی برنامه کاربردی از سایر برنامه‌های کاربردی می‌باشد)	4.3
2017-0402[37]	افشای اطلاعات در EffectBundle.cpp	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده بدون مجوز	4.3
2017-0401[38]	افشای اطلاعات در EffectBundle.cpp از Qualcomm audio	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2017-0396[40]	افشای اطلاعات در EffectVisualizer.cpp	بی تاثیر	بی تاثیر	متوسط	-دسترسی به داده حساس بدون مجوز	4.3
2016-6762[49]	ترفیع در حقوق در کتابخانه libziparchive	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	6.8
2016-6754[50]	اجرای کد راه دور در Webview	جزئی	جزئی	متوسط	-اجرای کد دلخواه در زمان مرور وب سایت توسط کاربر -احتمال اجرای کد راه دور در یک پردازش غیرممتاز	6.8
2016-6703[51]	اجرای کد راه دور در یک کتابخانه زمان اجرای اندروید	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-6702[52]	اجرای کد راه دور در libjpeg	جزئی	جزئی	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	6.8
2016-3897[57]	کلاس WifiEnterpriseConfig	بی تاثیر	بی تاثیر	متوسط	-بدست آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش و رمز عبور موجود در مقدار بازگشتی از متد فراخوانی	4.3
2016-3896[58]	AOSP Mail و اطلاعات EmailAccountCacheProvider	بی تاثیر	بی تاثیر	متوسط	-بدست‌آوردن اطلاعات از طریق برنامه کاربردی مخدوش	4.3

2016-3837[68]	wifi_WifiNative.cpp	بی تاثیر	بی تاثیر	متوسط	-بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش (تامین آدرس MAC با کاراکترهای خیلی کم)	4.3
2016-3836[69]	سرویس SurfaceFlinger	بی تاثیر	بی تاثیر	متوسط	-بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-3835[70]	نشست امن در جزء mm-video-v4l2 venc	بی تاثیر	بی تاثیر	متوسط	-استفاده نادرست از اشاره‌گرهای هیپ -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-3834[71]	camera APIs	بی تاثیر	بی تاثیر	متوسط	-رد نمودن محدودیت دسترسی -بدست‌آوردن اطلاعات حساس درباره آدرس‌های بافر ANW از طریق برنامه کاربردی مخدوش	4.3
2016-3822[73]	exif.c استفاده‌شده در libjhead	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (دسترسی خارج از محدوده) از طریق داده EXIF مخدوش	7.5
2016-3761[74]	NfcService.java در NFC	بی تاثیر	بی تاثیر	کم	-بدست‌آوردن اطلاعات برنامه کاربردی پیش‌زمینه[101] حساس از طریق برنامه کاربردی پس‌زمینه مخدوش	2.1
2016-3744[76]	سرریز بافر در create_pbuf function در btif/src/btif_hh.c در بلوتوث	جزئی	جزئی	بالا	-بدست‌آوردن حقوق از طریق عملیات جفت‌سازی مخدوش	4.3
2016-2500[79]	Terminate گروه های پردازشی	بی تاثیر	بی تاثیر	متوسط	-بدست‌آوردن اطلاعات حساس از طریق برنامه مخدوش	4.3
2016-2499[80]	AudioSource.cpp	بی تاثیر	بی تاثیر	متوسط	-مقداردهی اولیه نادرست -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-2463[83]	سرریز عدد صحیح در جزء h264dec	جزئی	جزئی	کم	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	7.5
2016-2458[84]	عملیات ترکیبی در AOSP Mail	بی تاثیر	بی تاثیر	متوسط	-محدودسازی نامناسب الصاقات[102] و بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش توسط مهاجم	4.3
2016-2426[92]	جزء قالب‌کاری ContentService.java	بی تاثیر	بی تاثیر	متوسط	-عدم بررسی جهت مجوز GET_ACCOUNTS -بدست‌آوردن اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-1155[99]	تزریق سرآیند Http در کلاس URLConnection	جزئی	جزئی	کم	-اجرای اسکریپت‌های دلخواه یا مقداردهی مقادیر دلخواه را در کوکی‌ها[103]	7.5

[101] Foreground
[102] Attachments
[103] Cookies

2016-0850[100]	PAIRING_CONFLIC در بلوتوث	جزئی	جزئی	کم	-ردنمودن محدودیت‌های جفت‌سازی از طریق دستگاه مخدوش	5.8
2016-0831[104]	تابع getDeviceIdForPhone	بی تاثیر	بی تاثیر	متوسط	عدم بررسی مجوز READ_PHONE_STATE و دستیابی به اطلاعات حساس از طریق برنامه کاربردی مخدوش	4.3
2016-0829[105]	onTransact در IGBufConsumer.cpp	بی تاثیر	بی تاثیر	کم	-عدم مقداردهی اولیه برای ساختارداده‌ای معین -بدست‌آوردن اطلاعات حساس -ردنمودن حفاظت بوسیله راه‌اندازی فعالیت QUEUE_BUFFER	5
2016-0828[106]	onTransact در IGBufConsumer.cpp	بی تاثیر	بی تاثیر	کم	عدم مقداردهی اولیه متغیر و بدست‌آوردن اطلاعات حساس توسط مهاجم -ردنمودن مکانیزم حفاظت بوسیله راه‌اندازی فعالیت ATTACH_BUFFER	5

آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1 با محرمانگی کامل در جدول 19 بیان شده است.

جدول 19- آسیب‌پذیری‌های موجود در سیستم‌عامل اندروید 5.1 با محرمانگی کامل

شماره شناسه	نام آسیب‌پذیری	صحت	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2017-0596[6]	ترفیع در حقوق libstagefright	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0594[7]	ترفیع در حقوق SoftAACEncoder2.cpp	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز -بدست‌آوردن توانایی ترفیع‌یافته	9.3
2017-0592[8]	اجرای کد راه دور FLACExtractor.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0592[9]	اجرای کد راه دور در libhevc	کامل	کامل	متوسط	- خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0588[10]	اجرای کد راه دور در id3/ID3.cpp	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده با استفاده از فایل مخدوش	9.3
2017-0553[15]	ترفیع در حقوق در libnl	کامل	کامل	بالا	-اجرای کد دلخواه در سرویس WiFi	7.6
2017-0546[17]	ترفیع در حقوق در SurfaceFlinger	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0545[18]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0544[19]	ترفیع در حقوق در CameraBase	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3
2017-0541[20]	اجرای کد راه دور در sonivox	کامل	کامل	متوسط	-خرابی حافظه در طول پردازش داده	9.3

	- احتمال اجرای کد راه دور در داخل مفهوم پردازش Mediaserver					
2017-0540[21]	اجرای کد راه دور در libhevc	کامل	کامل	متوسط	- خرابی حافظه در طول پردازش داده از طریق فایل مخدوش - حیاتی بودن بدلیل احتمال اجرای کد راه دور در داخل پردازش Mediaserver	9.3
2017-0480[28]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی به توانایی‌های ترفیع‌یافته	9.3
2017-0475[30]	ترفیع در حقوق در recovery verifier	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم هسته -حیاتی بودن بدلیل احتمال مخرب بودن دائمی دستگاه - سبب پاک‌سازی و قرارگیری مجدد سیستم عامل برای ترمیم دستگاه	9.3
2017-0419[35]	ترفیع در حقوق در Audioserver	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	9.3
2017-0410[36]	ترفیع در حقوق در قالب‌کاری API	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز - بدست‌آوردن دسترسی محلی به توانایی‌های ترفیع‌یافته	9.3
2017-0381[39]	افشای اطلاعات در NLSF_stabilize.c	کامل	کامل	متوسط	-دسترسی به داده حساس بدون مجوز	9.3
2016-6772[45]	ترفیع در حقوق در Wi-Fi	کامل	کامل	متوسط	-اجرای کد دلخواه در مفهوم پردازش ممتاز	9.3
2016-3921[54]	FrameworkListener.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3916[55]	camera_metadata.c	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3910[56]	TriggerHwService.cpp	کامل	کامل	متوسط	-دستیابی به حقوق از طریق برنامه کاربردی مخدوش	9.3
2016-3890[59]	JDWP در adb/sockets.cpp	کامل	کامل	متوسط	-بستن سوکت به شکل نادرست -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	9.3
2016-3885[60]	debuggerd.cpp از Debuggerd	کامل	کامل	متوسط	-کاربرد نادرست بین عملیات PTRACE_ATTACH و نخ -بدست‌آوردن حقوق از طریق برنامه مخدوش	9.3
2016-3872[63]	SoftVPX.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3871[64]	سریز بافر در SoftMP3.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3870[65]	OMXComponent.cpp	کامل	کامل	متوسط	-بدست‌آوردن حقوق مازاد، از طریق برنامه کاربردی مخدوش	9.3
2016-3861[66]	LibUtils	کامل	کامل	متوسط	-استفاده نادرست از تبدیلات مابین کدگذاری	9.3

	کاراکتری Unicode و سایر کدگذاری‌ها -اجرای کد دلخواه -سبب منع‌سرویس -سریز بافر مبتنی بر هیپ					
10	-شناسایی نادرست استفاده‌های مجدد[۱۰۴] از نشست[105] -اجرای کد دلخواه	کم	کامل	کامل	Conscrypt	2016-3840[67]
10	-بدست‌آوردن حقوق، از طریق برنامه کاربردی مخدوش	کم	کامل	کامل	Use-after-free در جزء mm-video-v4l2 venc	2016-3747[75]
9.3	-اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	متوسط	کامل	کامل	سرریز عدد صحیح در h264bsd_storage.c	2016-2507[77]
10	-عدم اعتبارسنجی آفست معین -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	کم	کامل	کامل	DRMExtractor.cpp از libstagefright	2016-2506[78]
9.3	-اجرای کد دلخواه یا سبب منع سرویس از طریق فایل mkv مخدوش	متوسط	کامل	کامل	libvpx از libwebm	2016-2464[82]
9.3	-عدم اعتبارسنجی اندازه بافر -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	SoftAMR.cpp	2016-2452[86]
9.3	-عدم اعتبارسنجی شناسه‌های قالب[۱۰۶] -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	Camera3Device.cpp	2016-2449[87]
9.3	-استفاده نادرست از ارجاعات شیء -بدست‌آوردن حقوق مازاد از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	IPCThreadState.cpp	2016-2440[88]
9.3	-بدست‌آوردن حقوق از طریق یک برنامه کاربردی شامل نام سمبل مخدوش	متوسط	کامل	کامل	Backtrace.cpp در debuggerd	2016-2430[89]
10	-ممانعت از عملیات آزاد بر روی حافظه بدون مقداردهی اولیه -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه هیپ) از طریق فایل رسانه مخدوش	کم	کامل	کامل	stream_decoder.c	2016-2429[90]
10	-محدودسازی نامناسب تعداد نخ‌ها -اجرای کد دلخواه یا یا سبب منع‌سرویس (خرابی حافظه پشته) از طریق فایل رسانه مخدوش	کم	کامل	کامل	aacdec_drc.cpp	2016-2428[91]
9.3	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	متوسط	کامل	کامل	rootdir/init.rc	2016-2420[94]
10	-عدم مقداردهی اولیه ساختمان داده پارامتر -بدست‌آوردن اطلاعات حساس از حافظه پردازش -ردنمودن مکانیزم حفاظت	کم	کامل	کامل	IOMX.cpp	2016-2417[95]
10	-عدم بررسی برای مجوز android	کم	کامل	کامل	BuffQueConsumer.cpp	2016-2416[96]

[104] Reuse
[105] Session
[106] Template IDs

	permission DUMP -بدست‌آوردن اطلاعات حساس -ردنمودن مکانیزم حفاظت از طریق درخواست dump					
2016-2415[97]	EasAutoDiscover.java	بی تاثیر	بی تاثیر	متوسط	در پیاده‌سازی Autodiscover از Exchange ActiveSync به مهاجمین اجازه می‌دهد تا اطلاعات حساسی را از برنامه کاربردی مخدوش بدست آورند که پاسخی جعلی برای درخواست GET راه‌اندازی می‌نماید.	7.1
2016-0849[101]	سریز عدد صحیح در SysUtil.c	کامل	کامل	کم	-دستیابی به حقوق از طریق برنامه کاربردی مخدوش	7.2
2016-0846[102]	IMemory.cpp	کامل	کامل	کم	-فرض نامناسب در اندازه هیپ -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	7.2
2016-0843[103]	Qualcomm performance-event manager	کامل	کامل	کم	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	7.2
2016-0826[107]	Libcameraservice	کامل	کامل	متوسط	-عدم نیاز به متد ICameraService:dump برای dump سرویس دوربین - بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوشی که مستقیماً dump می‌کند	9.3
2016-0804[112]	تابع notifyPreparedAndCleanup	کامل	کامل	کم	این تابع در GenericSource.cpp قرار دارد -مدیریت نادرست اشیای mDrmManagerClient -اجرای کد دلخواه یا سبب منع‌سرویس (خرابی حافظه) از طریق فایل رسانه مخدوش	10

3-13-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل اندروید ۵.۱ موجود در ایران، تلفن‌های همراه هوشمند و تلویزیون‌های هوشمند می‌باشند. در واقع اندروید به عنوان سیستم‌عاملی رایج بر روی تلفن‌های همراه هوشمند موجود در ایران می‌باشند. در این کار تمرکز بر روی تلویزیون‌های هوشمند می‌باشد. مورد استفاده از سیستم‌عامل اندروید 5.1 در تلویزیون‌های هوشمند موجود در ایران مربوط به برخی محصولات شرکت‌های Sony، Sharp، Snowa می‌باشند. تلویزیون‌های هوشمند Sony KD 55X8500D Smart BRAVIA Series LED TV، Sony KDL 43W800C BRAVIA Series Smart LED TV، Sony LED 4K TV 55X8500C، Sony KD 49X8300C Sony KDL 55W800 BRAVIA Series Smart LED TV، BRAVIA Series Smart LED TV، Sony 43X8000D، Sony KDL 55W650D Smart BRAVIA Series LED TV، Sony 49X8000D Forka Smart، Sony HDR 55X7000D 4K، Sony 55XD8505 Forka، Sony 65X9300D 3D 4K، Sony 4K TV

Sharp UHD ،Sony 65X8500D 4K HDR ،Sony TV 55XD8599 Forka Smart ،55X7000D Forka HDR ،Sharp 58UE630X ULTRA HD ،Sharp 50UE630X Forka Smart ،4K LED TV LC-50UE 1M Forka ،Snowa Smart SLD-50S44BLD ،Snowa SLD-43S44BLD Smart LED TV که از اندروید 5.1 به عنوان سیستم‌عامل بهره می‌برند، متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشند.

4- سیستم‌عامل تایزن

تایزن[۱۰۷] سیستم‌عاملی مبتنی بر هسته لینوکس است و کتابخانه های API GNU C لینوکس را پیاده‌سازی می‌کند. این سیستم‌عامل بر روی محدوده گسترده‌ای از دستگاه‌های تلفن همراه هوشمند، تبلت‌ها، دستگاه‌های خودروهای سرگرمی[۱۰۸] (IVI)، تلویزیون‌های هوشمند، دوربین‌های هوشمند، محاسبات پوشیدنی[۱۰۹] (مثل ساعت‌های مچی هوشمند)، پخش‌کننده‌های Blu-ray، چاپگرها و لوازم خانگی هوشمند (مثل یخچال‌وفریزر، روشنایی، ماشین لباسشویی، سیستم‌های تهویه مطبوع، اجاق و مایکروویو و جاروبرقی روباتیک) کار می‌کند. انجمن تایزن برای راهنمایی نقش صنعتی تایزن تشکیل شد که شامل جمع‌آوری نیازمندی‌ها[۱۱۰]، تعیین و تسهیل مدل‌های سرویس و بازاریابی صنعت کلی و آموزش می‌باشد. ریشه‌های تایزن به پلت‌فرم لینوکسی سامسونگ[۱۱۱] (SLP) و پروژه LiMo بر می‌گردد و در سال 2013 سامسونگ آنرا با پروژه Bada در داخل تایزن، ادغام کرد. در اولین هفته از اکتبر 2013، دوربین هوشمند NX300M سامسونگ به اولین محصول مشتری براساس تایزن، تبدیل شد. این محصول در کره جنوبی به مدت یک ماه فروخته شد و سپس برای پیش‌خرید در ایالات متحده در اوایل سال 2014 در دسترس قرار گرفت. اولین تبلت تایزن بوسیله Systena در ژوئن 2013 با یک پردازنده ARM 4 هسته‌ای 10 اینچی با رزلوشن 1920*1200 عرضه شد که در نهایت در اواخر اکتبر 2013 به عنوان یک بخشی از بسته توسعه اختصاصی برای ژاپن، روانه بازار شد. سامسونگ تلفن‌همراه هوشمند مبتنی بر تایزن خود را با نام Samsung-Z1 برای بازار هند در ژانویه 2015 عرضه کرد[117].

4-1- معماری سیستم

تایزن ابزار توسعه برنامه‌کاربردی را براساس کتابخانه‌های جاوااسکریپ JQuery و JQuery Mobile تامین می‌نماید. بسته توسعه نرم‌افزار به توسعه‌دهندگان اجازه می‌دهد تا از HTML5 و تکنولوژی‌های وب مرتبط استفاده نماید تا برنامه‌های کاربردی‌ای را بنویسند که بر روی دستگاه‌ها اجرا گردد. به عنوان نمونه OFono پشته تلفنی[۱۱۲]می‌باشد و Smack برای Sandbox برنامه‌های کاربردی وب HTML5 و سیستم پنجره‌ای X با کتابخانه‌های پایه Enlightenment استفاده‌شده است. تایزن تا نسخه 2.x از Wayland در نصب‌های IVI و از 3.0 بطور پیش‌فرض از Wayland بهره می‌برد. همچنین ZYpp به عنوان سیستم مدیریت بسته[۱۱۳] و ConnMan بر روی NetworkManager انتخاب‌شده‌اند[117].

---

[107] Tizen
[108] In-vehicle Infotainment Devices
[109] Wearable Computing
[110] Requirements Gathering
[111] Samsung Linux Platform
[112] Telephony Stack
[113] Package Management System

4-2- ریسک‌های امنیتی

در 3 آوریل 2017، Vice بر روی وب‌سایت Motherboard خودش گزارش داد که Amihai Neiderman، یک متخصص امنیتی اسرائیلی، بیش از 40 آسیب‌پذیری صفرروزه[۱۱۴] در کد تایزن پیدا کرد که به مهاجمین اجازه دسترسی راه دور به انواع گسترده‌ای از محصولات سامسونگ فعلی را می‌دهد[117].

4-3- آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4

ارزیابی آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 براساس پارامترهای مطرح در ارزیابی (محرمانگی، صحت، دسترس‌پذیری و پیچیدگی دسترسی)، انجام شده است. آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت بی‌تاثیر در جدول 20 بیان شده است.

جدول 20- آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت بی‌تاثیر

شماره شناسه	نام آسیب‌پذیری	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2015-6251[118]	دوبل‌آزاد[۱۱۵]	جزئی	کم	سبب منع‌سرویس از طریق مدخل DistinguishedName (DN) در یک گواهی[۱۱۶]	5
2014-8564[119	تابع ansi_x963_export در gnutls_ecc.c از GnuTLS 3.x	جزئی	کم	سبب منع‌سرویس (نوشتن خارج از محدوده) از طریق گواهی رمزنگاری منحنی بیضوی[۱۱۷] ECC یا درخواست‌های امضای گواهی CSR مخدوش مرتبط با تولید شناسه‌های کلید	5
2017-5972[123]	پشته TCP در هسته لینوکس x.3	کامل	کم	-پیاده‌سازی نامناسب مکانیزم حفاظت کوکی SYN برای اتصال شبکه‌ای سریع - سبب منع‌سرویس(مصرف پردازنده) از طریق ارسال زیاد بسته‌های TCP SYN	7.8
2015-1350[133]	زیرسیستم VFS	جزئی	کم	-تامین مجموعه نامطمئنی از نیازمندی‌ها برای عملیات setattr - سبب منع‌سرویس(سلب قابلیت) از طریق فراخوانی‌های شکست‌خورده (فراخوانی‌هایی که باعث شکست می‌شود)	2.1
2010-5321[114]	نشر حافظه در videobuf-core.c در زیرسیستم videobuf	کامل	کم	- سبب منع‌سرویس (خرابی حافظه) بوسیله پوشش دسترسی mmap برای یک سری دستورات dev/video/	4.9

آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت جزئی در جدول 21 بیان شده است.

جدول 21- آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت جزئی

شماره شناسه	نام آسیب‌پذیری	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز

[114] Zero-day
[115] Double Free
[116] Certificate
[117] Elliptic Curve Cryptography

2015-3164[120]	احرازهویت در XWayland	بی تاثیر	کم	-شروع کارگذار[118] بدون‌احرازهویت[119] -خواندن یا ارسال اطلاعات از مشتری‌های[120] X11 دلخواه از طریق سوکت یونیکس[121]	3.6
2014-8103[121]	کارگذار X.org (با نام مستعار xserver و xorg server)	جزئی	کم	- منع‌سرویس (نوشتن خارج از محدوده) یا احتمالاً اجرای کد دلخواه از طریق طول یا مقدار اندیس مخدوش برای توابع sproc_dri3_query_version، sproc_dri3_open، sproc_dri3_pixmap_from_buffer، sproc_dri3_buffer_from_pixmap، sproc_dri3_fence_from_fd، sproc_dri3_fd_from_fence، proc_present_query_capabilities، sproc_present_query_version، sproc_present_pixmap، sproc_present_notify_msc، sproc_present_select_input، sproc_present_query_capabilities توسط کاربران تصدیق‌شده[122] راه دور - تاثیر این آسیب‌پذیری بر روی احرازهویت به شکل سیستم تنها می‌باشد. آسیب‌پذیری نیازمند مهاجمی می‌باشد که به سیستم وارد شده باشد[123] (از جمله در خط دستور یا از طریق نشست رومیزی یا واسط وب)	6.5
2014-8094[122]	سرریز عدد صحیح در تابع ProcDRI2GetBuffers از توسعه DRI2 در کارگذار X.Org	جزئی	کم	- سبب منع‌سرویس(خرابی) یا احتمالاً اجرای کد دلخواه از طریق یک درخواست مخدوش -راه‌اندازی[124] خواندن یا نوشتن خارج از محدوده - تاثیر این آسیب‌پذیری بر روی احرازهویت به شکل سیستم تنها می‌باشد. آسیب‌پذیری نیازمند مهاجمی می‌باشد که به سیستم وارد شده باشد[125] (از جمله در خط دستور یا از طریق نشست رومیزی یا واسط وب)	6.5
2016-5870[124]	تابع msm_ipc_router_close در ipc_router_socket.c در جزء ipc_router	جزئی	کم	سبب منع‌سرویس(ارجاع مجدد اشاره‌گر تهی) یا تاثیر دیگر با راه‌اندازی شکستی از فراخوانی سیستمی AF_MSM_IPC	4.6
2016-5343[126]	voice_svc.c در درایور سرویس صدای QDSP6v2	جزئی	کم	سبب منع‌سرویس(ارجاع مجدد اشاره‌گر تهی) یا تاثیر دیگر از طریق درخواست نوشتن	7.5
2015-0572[135]	شرایط race در adsprpc.c و adsprpc_compat.c در	جزئی	کم	سبب منع‌سرویس (نوشتن مقدار صفر) یا تاثیر دیگر از طریق فراخوانی ioctl IOCTL_INVOKE_FD	7.5

[118] Server
[119] Non-authenticating Mode
[120] Clients
[121] Unix Sockets
[122] Authenticated Users
[123] Login
[124] Trigger
[125] Login

	درایور ADSPRPC				

آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت کامل در جدول 22 بیان شده است.

جدول 22- آسیب‌پذیری‌های موجود در سیستم‌عامل تایزن 2.4 با محرمانگی و صحت کامل

شماره شناسه	نام آسیب‌پذیری	دسترس پذیری	پیچیدگی دسترسی	توضیحات	امتیاز
2016-5344[125]	سرریز بافر در درایور MDSS	کامل	کم	سبب منع‌سرویس(ارجاع مجدد اشاره‌گر تهی) یا تاثیر دیگر از طریق مقدار بزرگ (مرتبط با mdss_fb.c ،mdss_compat_utils.c، mdss_rotator.c)	10
2016-5342[127]	سرریز بافر مبتنی بر هیپ در تابع wcnss_wlan_write در wcnss_wlan.c در درایور دستگاه wcnss_wlan	کامل	کم	سبب منع‌سرویس(ارجاع مجدد اشاره‌گر تهی) یا تاثیر دیگر از طریق درخواست نوشتن نوشتن بر روی dev/wcnss_wlan/ با یک مقدار داده غیرمنتظره	7.2
2016-5340[128]	تابع is_ashmem_file در ashmem.c	کامل	کم	-اعتبارسنجی نادرست اشاره گر در داخل ماژول‌های گرافیکی لینوکس KGSL -رد نمودن محدودیت‌های دسترسی از طریق استفاده از رشته /ashmem به عنوان نام dentry	7.2
2016-2067[129]	kgsl.c در درایور گرافیکی MSM	کامل	متوسط	-کاربرد نادرست پرچمGPUREADONLY -بدست‌آوردن حقوق از طریق پوشش نگاشت‌های خواندن/نوشتن تصادفی	9.3
2016-2066[130]	خطای علامت‌داری عدد صحیح در درایور صدای MSM QDSP6	کامل	متوسط	-بدست‌آوردن حقوقی یا سبب منع‌سرویس (خرابی حافظه) از طریق برنامه‌کاربردی مخدوش	9.3
2016-2063[131]	سرریز بافر مبتنی بر پشته در تابع supply_lm_input_write در supply_lm_core.c در درایور حرارتی MSM	کامل	کم	سبب منع‌سرویس(ارجاع مجدد اشاره‌گر تهی) یا تاثیر دیگر از طریق برنامه کاربردی مخدوش(ارسال مقادیر بزرگتری از داده از طریق واسط debugfs)	10
2016-2061[132]	خطای علامت‌داری عدد صحیح در درایور ویدیویی MSM V4L2	کامل	کم	-بدست‌آوردن یا سبب منع‌سرویس (سرریز آرایه و خرابی حافظه) از طریق برنامه‌کاربردی مخدوش(راه‌اندازی فراخوانی msm_isp_axi_create_stream)	9.3
2015-0573[134]	broadcast/tsc.c از درایور TSC	کامل	کم	سبب منع‌سرویس (ارجاع مجدد اشاره‌گر نامعتبر) یا تاثیر نامشخص از طریق برنامه‌کاربردی مخدوش (TSC_GET_CARD_STATUS ioctl را فراخوانی می‌نماید)	10
2015-0571[136]	درایور WLAN (با نام مستعار WiFi)	کامل	متوسط	-عدم اعتبارسنجی مجوز برای فراخوانی SET IOCTL -بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش	9.3
2015-0570[137]	سرریز بافر مبتنی بر پشته در پیاده‌سازی SET_WPS_IE IOCTL در	کامل	متوسط	-بدست‌آوردن حقوق از طریق برنامه کاربردی	9.3

	wlan_hdd_hostapd.c در WLAN (با نام مستعار WiFi)			مخدوش (استفاده از WPS IE)	
2015-0569[138]	سرریز بافر مبتنی بر هیپ در پیاده‌سازی IOCTL توسعه‌های بی‌سیم در wlan_hdd_wext.c در درایور WLAN(با نام مستعار WiFi)	کامل	متوسط	-بدست‌آوردن حقوق از طریق برنامه کاربردی مخدوش (حقوق، فیلترسازی بسته می‌باشد)	9.3
2015-0568[139]	Use-after-free در تابع msm_set_crop در msm_camera.c در درایور دوربین MSM	کامل	کم	-بدست‌آوردن حقوق یا سبب منع‌سرویس(خرابی حافظه) از طریق برنامه‌کاربردی (فراخوانی ioctl مخدوش می‌باشد)	7.2
2014-9410[140]	تابع vfe31_proc_general در msm_vfe31.c در درایور MSM-VFE31	کامل	کم	-عدم اعتبارسنجی شناسه -بدست‌آوردن حقوق - منع‌سرویس(خرابی حافظه) از طریق برنامه‌کاربردی (فراخوانی ioctl مخدوش می‌باشد)	7.2

4-3-1- دستگاه‌های آسیب‌پذیر پرکاربرد موجود در ایران

دستگاه‌های پرکاربرد استفاده‌کننده از سیستم‌عامل تایزن 2.4 موجود در ایران، تلویزیون‌های هوشمند می‌باشند. مورد استفاده از سیستم‌عامل تایزن 2.4 در تلویزیون‌های هوشمند موجود در ایران مربوط به برخی محصولات شرکت Samsung می‌باشند. تلویزیون‌های هوشمند Samsung 88KS10000، Samsung 78KS9995، Samsung 65MS9995، Samsung 65KS8985، Samsung 70KU7970، Samsung 65KU7975، Samsung 60KS8980، Samsung 55KS8985، Samsung 49M6960 که از تایزن 2.4 به عنوان سیستم‌عامل بهره می‌برند، متاثر از آسیب‌پذیری‌های ذکرشده در بخش قبل می‌باشند.

5- منابع و مراجع

[1] Vulnerability Details: CVE-2011-2409 , https://www.cvedetails.com/cve/CVE-2011-2409/

[2] Vulnerability Details: CVE-2011-2408 , https://www.cvedetails.com/cve/CVE-2011-2408/

[3] Vulnerability Details: CVE-2017-0603 , https://www.cvedetails.com/cve/CVE-2017-0603/

[4] Vulnerability Details: CVE-2017-0602, https://www.cvedetails.com/cve/CVE-2017-0602/

[5] Vulnerability Details: CVE-2017-0598, https://www.cvedetails.com/cve/CVE-2017-0598/

[6] Vulnerability Details: CVE-2017-0596, https://www.cvedetails.com/cve/CVE-2017-0596/

[7] Vulnerability Details: CVE-2017-0594, https://www.cvedetails.com/cve/CVE-2017-0594/

[8] Vulnerability Details: CVE-2017-0592, https://www.cvedetails.com/cve/CVE-2017-0592/

[9] Vulnerability Details: CVE-2017-0590, https://www.cvedetails.com/cve/CVE-2017-0590/

[10] Vulnerability Details: CVE-2017-0588, https://www.cvedetails.com/cve/CVE-2017-0588/

[11] Vulnerability Details: CVE-2017-0560, https://www.cvedetails.com/cve/CVE-2017-0560/

[12] Vulnerability Details: CVE-2017-0559, https://www.cvedetails.com/cve/CVE-2017-0559/

[13] Vulnerability Details: CVE-2017-0558, https://www.cvedetails.com/cve/CVE-2017-0558/

[14] Vulnerability Details: CVE-2017-0554, https://www.cvedetails.com/cve/CVE-2017-0554/

[15] Vulnerability Details: CVE-2017-0553, https://www.cvedetails.com/cve/CVE-2017-0553/

[16] Vulnerability Details: CVE-2017-0547, https://www.cvedetails.com/cve/CVE-2017-0547/

[17] Vulnerability Details: CVE-2017-0546, https://www.cvedetails.com/cve/CVE-2017-0546/

[18] Vulnerability Details: CVE-2017-0545, https://www.cvedetails.com/cve/CVE-2017-0545/

[19] Vulnerability Details: CVE-2017-0544, https://www.cvedetails.com/cve/CVE-2017-0544/

[20] Vulnerability Details: CVE-2017-0541, https://www.cvedetails.com/cve/CVE-2017-0541/

[21] Vulnerability Details: CVE-2017-0540, https://www.cvedetails.com/cve/CVE-2017-0540/

[22] Vulnerability Details: CVE-2017-0499, https://www.cvedetails.com/cve/CVE-2017-0499/

[23] Vulnerability Details: CVE-2017-0498, https://www.cvedetails.com/cve/CVE-2017-0498/

[24] Vulnerability Details: CVE-2017-0496, https://www.cvedetails.com/cve/CVE-2017-0496/

[25] Vulnerability Details: CVE-2017-0491, https://www.cvedetails.com/cve/CVE-2017-0491/

[26] Vulnerability Details: CVE-2017-0489, https://www.cvedetails.com/cve/CVE-2017-0489/

[27] Vulnerability Details: CVE-2017-0483, https://www.cvedetails.com/cve/CVE-2017-0483/

[28] Vulnerability Details: CVE-2017-0480, https://www.cvedetails.com/cve/CVE-2017-0480/

[29] Vulnerability Details: CVE-2017-0478, https://www.cvedetails.com/cve/CVE-2017-0478/

[30] Vulnerability Details: CVE-2017-0475, https://www.cvedetails.com/cve/CVE-2017-0475/

[31] Vulnerability Details: CVE-2017-0425, https://www.cvedetails.com/cve/CVE-2017-0425/

[32] Vulnerability Details: CVE-2017-0422, https://www.cvedetails.com/cve/CVE-2017-0422/

[33] Vulnerability Details: CVE-2017-0421, https://www.cvedetails.com/cve/CVE-2017-0421/

[34] Vulnerability Details: CVE-2017-0420, https://www.cvedetails.com/cve/CVE-2017-0420/

[35] Vulnerability Details: CVE-2017-0419, https://www.cvedetails.com/cve/CVE-2017-0419/

[36] Vulnerability Details: CVE-2017-0410, https://www.cvedetails.com/cve/CVE-2017-0410/

[37] Vulnerability Details: CVE-2017-0402, https://www.cvedetails.com/cve/CVE-2017-0402/

[38] Vulnerability Details: CVE-2017-0401, https://www.cvedetails.com/cve/CVE-2017-0401/

[39] Vulnerability Details: CVE-2017-0381, https://www.cvedetails.com/cve/CVE-2017-0381/

[40] Vulnerability Details: CVE-2017-0396, https://www.cvedetails.com/cve/CVE-2017-0396/

[41] Vulnerability Details: CVE-2017-0395, https://www.cvedetails.com/cve/CVE-2017-0395/

[42] Vulnerability Details: CVE-2017-0394, https://www.cvedetails.com/cve/CVE-2017-0394/

[43] Vulnerability Details: CVE-2017-0393, https://www.cvedetails.com/cve/CVE-2017-0393/

[44] Vulnerability Details: CVE-2017-0390, https://www.cvedetails.com/cve/CVE-2017-0390/

[45] Vulnerability Details: CVE-2016-6772, https://www.cvedetails.com/cve/CVE-2016-6772/

[46] Vulnerability Details: CVE-2016-6769, https://www.cvedetails.com/cve/CVE-2016-6769/

[47] Vulnerability Details: CVE-2016-6766, https://www.cvedetails.com/cve/CVE-2016-6766/

[48] Vulnerability Details: CVE-2016-6763, https://www.cvedetails.com/cve/CVE-2016-6763/

[49] Vulnerability Details: CVE-2016-6762, https://www.cvedetails.com/cve/CVE-2016-6762/

[50] Vulnerability Details: CVE-2016-6754, https://www.cvedetails.com/cve/CVE-2016-6754/

[51] Vulnerability Details: CVE-2016-6703, https://www.cvedetails.com/cve/CVE-2016-6703/

[52] Vulnerability Details: CVE-2016-6702, https://www.cvedetails.com/cve/CVE-2016-6702/

[53] Vulnerability Details: CVE-2016-5348, https://www.cvedetails.com/cve/CVE-2016-5348/

[54] Vulnerability Details: CVE-2016-3921, https://www.cvedetails.com/cve/CVE-2016-3921/

[55] Vulnerability Details: CVE-2016-3916, https://www.cvedetails.com/cve/CVE-2016-3916/

[56] Vulnerability Details: CVE-2016-3910, https://www.cvedetails.com/cve/CVE-2016-3910/

[57] Vulnerability Details: CVE-2016-3897, https://www.cvedetails.com/cve/CVE-2016-3897/

[58] Vulnerability Details: CVE-2016-3896, https://www.cvedetails.com/cve/CVE-2016-3896/

[59] Vulnerability Details: CVE-2016-3890, https://www.cvedetails.com/cve/CVE-2016-3890/

[60] Vulnerability Details: CVE-2016-3885, https://www.cvedetails.com/cve/CVE-2016-3885/

[61] Vulnerability Details: CVE-2016-3881, https://www.cvedetails.com/cve/CVE-2016-3881/

[62] Vulnerability Details: CVE-2016-3879, https://www.cvedetails.com/cve/CVE-2016-3879/

[63] Vulnerability Details: CVE-2016-3872, https://www.cvedetails.com/cve/CVE-2016-3872/

[64] Vulnerability Details: CVE-2016-3871, https://www.cvedetails.com/cve/CVE-2016-3871/

[65] Vulnerability Details: CVE-2016-3870, https://www.cvedetails.com/cve/CVE-2016-3870/

[66] Vulnerability Details: CVE-2016-3861, https://www.cvedetails.com/cve/CVE-2016-3861/

[67] Vulnerability Details: CVE-2016-3840, https://www.cvedetails.com/cve/CVE-2016-3840/

[68] Vulnerability Details: CVE-2016-3837, https://www.cvedetails.com/cve/CVE-2016-3837/

[69] Vulnerability Details: CVE-2016-3836, https://www.cvedetails.com/cve/CVE-2016-3836/

[70] Vulnerability Details: CVE-2016-3835, https://www.cvedetails.com/cve/CVE-2016-3835/

[71] Vulnerability Details: CVE-2016-3834, https://www.cvedetails.com/cve/CVE-2016-3834/

[72] Vulnerability Details: CVE-2016-3831, https://www.cvedetails.com/cve/CVE-2016-3831/

[73] Vulnerability Details: CVE-2016-3822, https://www.cvedetails.com/cve/CVE-2016-3822/

[74] Vulnerability Details: CVE-2016-3761, https://www.cvedetails.com/cve/CVE-2016-3761/

[75] Vulnerability Details: CVE-2016-3747, https://www.cvedetails.com/cve/CVE-2016-3747/

[76] Vulnerability Details: CVE-2016-3744, https://www.cvedetails.com/cve/CVE-2016-3744/

[77] Vulnerability Details: CVE-2016-2507, https://www.cvedetails.com/cve/CVE-2016-2507/

[78] Vulnerability Details: CVE-2016-2506, https://www.cvedetails.com/cve/CVE-2016-2506/

[79] Vulnerability Details: CVE-2016-2500, https://www.cvedetails.com/cve/CVE-2016-2500/

[80] Vulnerability Details: CVE-2016-2499, https://www.cvedetails.com/cve/CVE-2016-2499/

[81] Vulnerability Details: CVE-2016-2495, https://www.cvedetails.com/cve/CVE-2016-2495/

[82] Vulnerability Details: CVE-2016-2464, https://www.cvedetails.com/cve/CVE-2016-2464/

[83] Vulnerability Details: CVE-2016-2463, https://www.cvedetails.com/cve/CVE-2016-2463/

[84] Vulnerability Details: CVE-2016-2458, https://www.cvedetails.com/cve/CVE-2016-2458/

[85] Vulnerability Details: CVE-2016-2457, https://www.cvedetails.com/cve/CVE-2016-2457/

[86] Vulnerability Details: CVE-2016-2452, https://www.cvedetails.com/cve/CVE-2016-2452/

[87] Vulnerability Details: CVE-2016-2449, https://www.cvedetails.com/cve/CVE-2016-2449/

[88] Vulnerability Details: CVE-2016-2440, https://www.cvedetails.com/cve/CVE-2016-2440/

[89] Vulnerability Details: CVE-2016-2430, https://www.cvedetails.com/cve/CVE-2016-2430/

[90] Vulnerability Details: CVE-2016-2429, https://www.cvedetails.com/cve/CVE-2016-2429/

[91] Vulnerability Details: CVE-2016-2428, https://www.cvedetails.com/cve/CVE-2016-2428/

[92] Vulnerability Details: CVE-2016-2426, https://www.cvedetails.com/cve/CVE-2016-2426/

[93] Vulnerability Details: CVE-2016-2424, https://www.cvedetails.com/cve/CVE-2016-2424/

[94] Vulnerability Details: CVE-2016-2420, https://www.cvedetails.com/cve/CVE-2016-2420/

[95] Vulnerability Details: CVE-2016-2417, https://www.cvedetails.com/cve/CVE-2016-2417/

[96] Vulnerability Details: CVE-2016-2416, https://www.cvedetails.com/cve/CVE-2016-2416/

[97] Vulnerability Details: CVE-2016-2415, https://www.cvedetails.com/cve/CVE-2016-2415/

[98] Vulnerability Details: CVE-2016-2414, https://www.cvedetails.com/cve/CVE-2016-2414/

[99] Vulnerability Details: CVE-2016-1155, https://www.cvedetails.com/cve/CVE-2016-1155/

[100] Vulnerability Details: CVE-2016-0850, https://www.cvedetails.com/cve/CVE-2016-0850/

[101] Vulnerability Details: CVE-2016-0849, https://www.cvedetails.com/cve/CVE-2016-0849/

[102] Vulnerability Details: CVE-2016-0846, https://www.cvedetails.com/cve/CVE-2016-0846/

[103] Vulnerability Details: CVE-2016-0843, https://www.cvedetails.com/cve/CVE-2016-0843/

[104] Vulnerability Details: CVE-2016-0831, https://www.cvedetails.com/cve/CVE-2016-0831/

[105] Vulnerability Details: CVE-2016-0829, https://www.cvedetails.com/cve/CVE-2016-0829/

[106] Vulnerability Details: CVE-2016-0828, https://www.cvedetails.com/cve/CVE-2016-0828/

[107] Vulnerability Details: CVE-2016-0826, https://www.cvedetails.com/cve/CVE-2016-0826/

[108] Vulnerability Details: CVE-2016-0818, https://www.cvedetails.com/cve/CVE-2016-0818/

[109] Vulnerability Details: CVE-2016-0813, https://www.cvedetails.com/cve/CVE-2016-0813/

[110] Vulnerability Details: CVE-2016-0812, https://www.cvedetails.com/cve/CVE-2016-0812/

[111] Vulnerability Details: CVE-2016-0808, https://www.cvedetails.com/cve/CVE-2016-0808/

[112] Vulnerability Details: CVE-2016-0804, https://www.cvedetails.com/cve/CVE-2016-0804/

[113] Vulnerability Details: CVE-2016-0802, https://www.cvedetails.com/cve/CVE-2016-0802/

[114] Vulnerability Details: CVE-2015-6645, https://www.cvedetails.com/cve/CVE-2015-6645/

[115] WebOS, https://en.wikipedia.org/wiki/WebOS#cite_note-opc-45

[116] Android (operating system), https://en.wikipedia.org/wiki/Android_%28operating_system%29

[117] Tizen, https://en.wikipedia.org/wiki/Tizen

[118] Vulnerability Details: CVE-2015-6251, https://www.cvedetails.com/cve/CVE-2015-6251/

[119] Vulnerability Details: CVE-2014-8564, https://www.cvedetails.com/cve/CVE-2014-8564/

[120] Vulnerability Details: CVE-2015-3164, https://www.cvedetails.com/cve/CVE-2015-3164/

[121] Vulnerability Details: CVE-2014-8103, https://www.cvedetails.com/cve/CVE-2014-8103/

[122] Vulnerability Details: CVE-2014-8094, https://www.cvedetails.com/cve/CVE-2014-8094/

[123] Vulnerability Details: CVE-2017-5972, https://www.cvedetails.com/cve/CVE-2017-5972/

[124] Vulnerability Details: CVE-2016-5870, https://www.cvedetails.com/cve/CVE-2016-5870/

[125] Vulnerability Details: CVE-2016-5344, https://www.cvedetails.com/cve/CVE-2016-5344/

[126] Vulnerability Details: CVE-2016-5343, https://www.cvedetails.com/cve/CVE-2016-5343/

[127] Vulnerability Details: CVE-2016-5342, https://www.cvedetails.com/cve/CVE-2016-5342/

[128] Vulnerability Details: CVE-2016-5340, https://www.cvedetails.com/cve/CVE-2016-5340/

[129] Vulnerability Details: CVE-2016-2067, https://www.cvedetails.com/cve/CVE-2016-2067/

[130] Vulnerability Details: CVE-2016-2066, https://www.cvedetails.com/cve/CVE-2016-2066/

[131] Vulnerability Details: CVE-2016-2063, https://www.cvedetails.com/cve/CVE-2016-2063/

[132] Vulnerability Details: CVE-2016-2061, https://www.cvedetails.com/cve/CVE-2016-2061/

[133] Vulnerability Details: CVE-2015-1350, https://www.cvedetails.com/cve/CVE-2015-1350/

[134] Vulnerability Details: CVE-2015-0573, https://www.cvedetails.com/cve/CVE-2015-0573/

[135] Vulnerability Details: CVE-2015-0572, https://www.cvedetails.com/cve/CVE-2015-0572/

[136] Vulnerability Details: CVE-2015-0571, https://www.cvedetails.com/cve/CVE-2015-0571/

[137] Vulnerability Details: CVE-2015-0570, https://www.cvedetails.com/cve/CVE-2015-0570/

[138] Vulnerability Details: CVE-2015-0569, https://www.cvedetails.com/cve/CVE-2015-0569/

[139] Vulnerability Details: CVE-2015-0568, https://www.cvedetails.com/cve/CVE-2015-0568/

[140] Vulnerability Details: CVE-2014-9410, https://www.cvedetails.com/cve/CVE-2014-9410/

[141] Vulnerability Details: CVE-2010-5321, https://www.cvedetails.com/cve/CVE-2010-5321/