HOW SAFE ARE POPULAR APPS?

A Study of Critical Vulnerabilities and Why Consumers Should Care

ACI
The American Consumer Institute
Center for Citizen Research

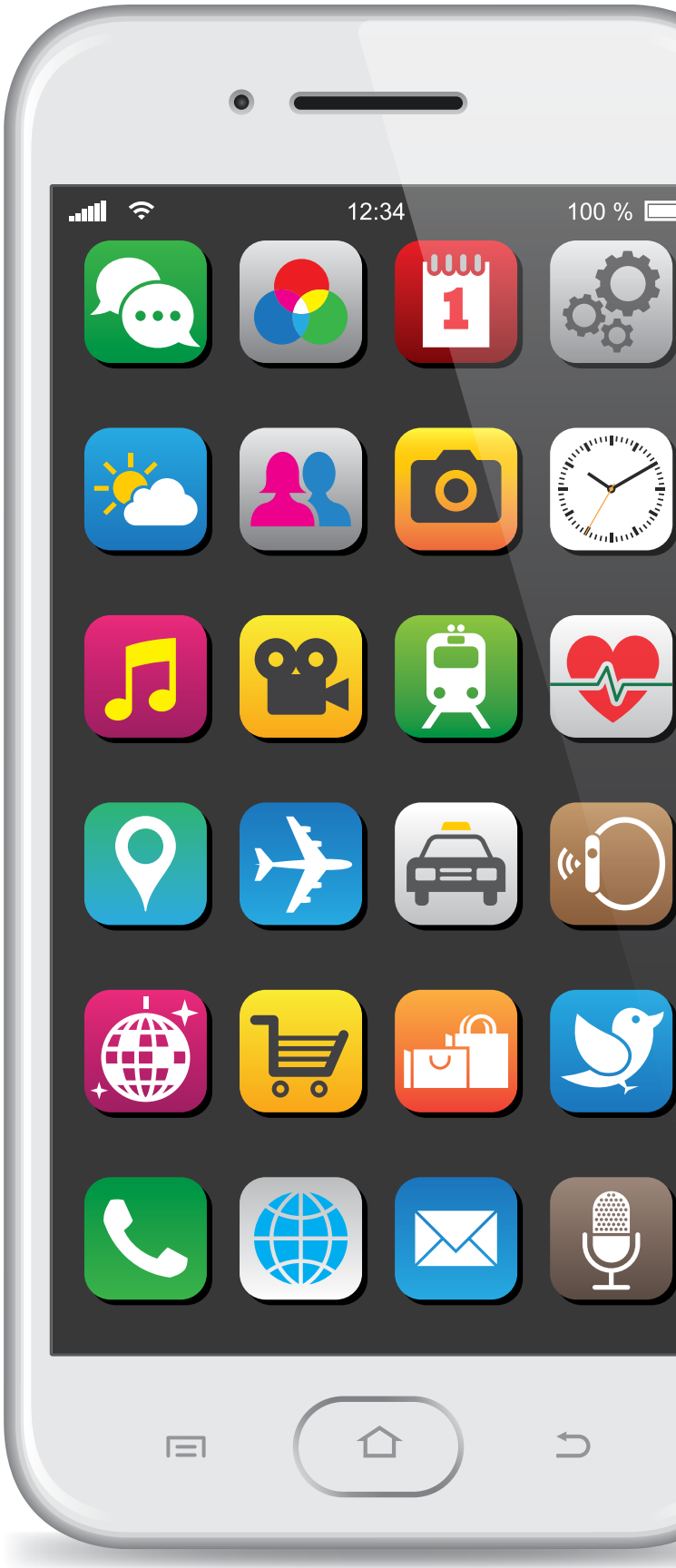
EXECUTIVE SUMMARY

Should consumers be concerned about their personal information – including credit card and location information – the next time they order an online pizza or use their ridesharing app? This report explores the security of the most popular Android apps and highlights the threats posed by the growing reliance of companies and American consumers on software that increasingly contains out-of-date, unsecured versions of open source components. With the annual cost of cybercrime expected to reach $2 trillion by 2019, this problem has not attracted the attention it deserves.[1]

The use of open source code has grown across all industries in recent years, allowing companies to lower development costs, bring their products to market faster, and accelerate innovation. Despite these advantages, open source code has certain characteristics that make it particularly attractive to hackers.

To gain a deeper understanding of open source vulnerabilities, this report scrutinizes 330 of the most popular Android apps in the U.S., drawn from 33 different categories. Using Insignary's Clarity tool, these common apps were analyzed (scanned) for known, preventable security vulnerabilities. Of the sample, 105 apps (32% of the total) were identified to contain vulnerabilities across a number of severity levels – critical, high, medium and low risk – totaling 1,978 vulnerabilities. In effect, the results found an average of 6 vulnerabilities per app over the entire sample -- or an alarming 19 vulnerabilities per app for the identified 105 apps.

Among the detected vulnerabilities, 43% are considered critical or high risk by the National Vulnerability Database. While all categories of apps contained a spectrum of security vulnerabilities, critical vulnerabilities were most common among libraries and demo, entertainment and finance apps. Vulnerabilities are designated as critical when little knowledge or skill is required to exploit them, and they can entirely compromise devices and networks.



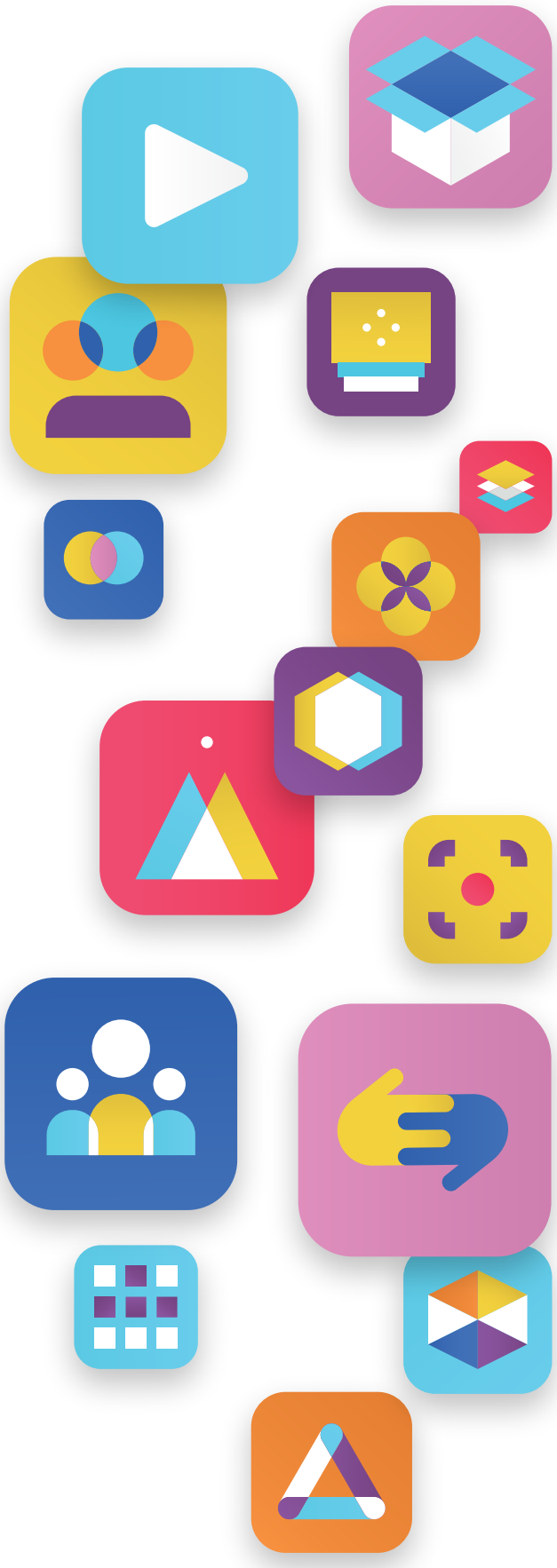
1 Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," Forbes, January 16, 2016, www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#f4bae343a913.

Critical vulnerabilities were found in many common applications, including some of the most popular banking, event ticket purchasing and travel apps, according to the Clarity scan results. Scans also identified high vulnerabilities among some of the most well-known sports apps, as well as popular dating, game, social media and food delivery apps. The problem, unnoticed by the general public, appears to be pervasive and could be present on most consumer devices.

These findings corroborate the results of previous studies and underline the need for more vigilance by app developers and consumers to prevent serious attacks. At the same time, companies, as well as state and local governments, are purchasing off-the-shelf applications, custom software and firmware that increasingly contain open source software components that harbor known security vulnerabilities.

As software's role in our lives continues to grow, cyberattacks are becoming more far-reaching and consequential than ever before. Innovation in self-driving automobiles, medical electronics and Internet of Things (IoT) devices are primarily built on a core of open source code. Leaving this technology vulnerable to hacks could have life-threatening consequences. In light of these risks, companies that unknowingly use out-of-date and unsecure open source components must be more diligent in countering these threats.

We recommend that software providers take more proactive steps to update their code for known vulnerabilities and notify their customers to do the same.



A TARGET-RICH ENVIRONMENT FOR HACKERS

The annual cost of cybercrime damage to consumers, companies and governments is expected to reach $2 trillion by 2019 – up from $500 billion in 2016.[2] About 20% of small to mid-sized companies have suffered a cyberattack. These estimates ignore the upheaval of personal anxieties and behavioral changes as we respond to cyber-fears. They also ignore the potentially calamitous damages from cyberwarfare mounted against our critical infrastructure.

According to one company that specializes in open source security, about 20% of the most popular Android software apps in the Google Play Store contain open source components known to harbor security vulnerabilities ready for exploitation by hackers.[3] A large portion of the low-cost devices that constitute IoT devices – the new wave of interconnected devices and machine-to-machine applications – have either no security provisions or were sold without the makers' commitment to provide security updates. Parts of our critical infrastructure have inadequate hardware and software security provisions, leaving consumers, businesses, and governments open to attacks with disastrous results.

Remember the Equifax hack? The attack, which began in May of 2017 and was disclosed four months later, was facilitated by a vulnerability in an open source software package. On March 8, 2017, the U.S. Department of Homeland Security sent out a notice of the need to patch a particular vulnerability in certain versions of Apache Struts.[4] Equifax knew of this particular vulnerability (CVE-2017-5638) and for unknown reasons did not patch the vulnerability.[5] By mid-May attackers had accessed sensitive information of millions of American consumers. The attack was reported to have compromised the information of over 148 million U.S. consumers, nearly 700,000 U.K. residents, and more than 19,000 Canadians.[6] The resulting cost of the breach is expected to surge by $275 million this year, suggesting the incident could turn out to be the costliest hack in corporate history.[7]

The Equifax attack is not an isolated case.[8] The need for open source security management is increasingly becoming frontpage news. To increase awareness, the U.S. government sponsors the Common Vulnerabilities and Exposures (CVE) database, operated by the MITRE Corporation, and the National Vulnerability Database at the National Institute of Standards and Technology.[9] Yet many companies and organizations appear unaware or turn a blind eye to these security issues in their software, leaving consumers at risk.

This study seeks to better understand the magnitude of the problem. Conducting an analysis of the most currently used Android apps on consumer smartphones and smart devices allows us to better understand the extent to which software used in the United States is potentially exposed to known open source vulnerabilities. Specifically, the study

2 Ibid.

3 "Comprehensive Android Binary Scans Find Known Security Vulnerabilities in 1 Out of Every 5 of the 700 Most Popular Apps on Google Play Store," Insignary, April 24, 2018, www.insignary.com/android-binary-scans.

4 Struts is widely used by Fortune 100 companies, including Equifax, to build corporate websites. "2018 Open Source Security and Risk Analysis Report," BlackDuck by Synopsys Center for Open Source Research & Innovation, 2018, https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2018-ossra.pdf.

5 Ibid.

6 Fred Bals, "Open source: it's not the code, it's people," Techradar.pro, June 22, 2018, https://www.techradar.com/news/open-source-its-not-the-code-its-people.

7 John McCrank and Jim Finkle, "Equifax breach could be most costly in corporate history," Reuters, March 2, 2018, www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257.

8 Dennis Green, "If you shopped at these 15 stores in the last year, your data might have been stolen," Business Insider, July 1, 2018, www.businessinsider.com/data-breaches-2018-4.

9 The U.S. government funds and the MITRE Corporation operates a public database of software vulnerabilities (see cve.mitre.org). Each listed vulnerability is assigned a unique CVE identifier that contains information about a specific vulnerability's capacities and risks. The National Vulnerability Database, which is available to the public, uses a scoring system to measure the risk associated with each vulnerability, and it reports each vulnerability as either critical, high, medium or low risk (see https://nvd.nist.gov/vuln-metrics/cvss).

explores the degree to which applications harbor known security vulnerabilities, making them more susceptible to cybercrime and other online threats. Without addressing these known security flaws, consumer devices could be compromised, and data could be stolen, leading to malicious activity, identity theft, fraud or corporate espionage.

THE BENEFITS AND PERILS OF OPEN SOURCE

Open source code has grown in popularity over the years and is used by companies of all sizes, across all industries. A 2017 Forrester Research report highlighted open source code's preeminence in application development, with proprietary custom code comprising only 10% to 20% of applications.[10]

According to a 2017 BlackDuck report, open source is neither more nor less secure than custom code, but there are certain characteristics of open source that make its vulnerabilities particularly attractive to attackers.[11] These characteristics include:

- Open source is widely used in commercial applications, providing attackers with a target-rich environment;
- Unlike some commercial software for personal computers and smartphones, where updates are automatically "pushed" to users, IoT devices and smartphones leverage a "pull" support model, where users are responsible for keeping track of vulnerabilities as well as fixes and updates for the software they use;[12]
- If an organization is not aware of all the open source used in its code, it cannot properly defend against common attacks targeting known vulnerabilities; and
- Hackers can more easily exploit known open source security vulnerabilities because they are publicly published on the CVE database, providing a roadmap for exploiting code.

So why do companies keep using or even switch to open source software? The reasons are straightforward: open source lowers development costs, speeds time-to-market, and significantly accelerates innovation. In other words, using open source saves developers time and it saves companies and consumers money. Even though open source is an essential element in application development today, companies that do not protect their software applications from known open source vulnerabilities run the risk of disastrous consequences for both themselves and their customers.

STUDY METHODOLOGY

Consumers often receive automated notices that they need to protect their personal computers by installing operating system patches and virus updates, but do application developers do the same? To what extent are consumers downloading smartphone or smart device apps that harbor known risks?

This study seeks to explore the degree to which applications and software code are potentially being left unpatched for known risks, making them more susceptible to cybercrime and other online threats. Without addressing these known security flaws, consumer devices could be compromised, and data could be stolen, leading to malicious activity, identity theft, fraud or espionage.

The results presented here are based on a sample of 330 Android applications selected using well-accepted and rigorous statistical methods. To determine which applications to include in the sample, www.androidrank.org, the oldest online service tracking Google Play history data, was used. Included in the sample are the top-10 most popular Android applications in the following categories:

- art and design
- auto and vehicles
- beauty
- books and reference
- business
- comics

10 Amy DeMartine, "The Forrester Wave: Software Composition Analysis, Q1 2017," Forrester Research, February 23, 2017, www.blackducksoftware.com/sites/default/files/images/Downloads/Reports/USA/ForresterWave-Rpt.pdf.

11 "2017 Open Source Security and Risk Analysis," BlackDuck, https://www.blackducksoftware.com/open-source-security-risk-analysis-2017.

12 "2018 Open Source Security and Risk Analysis Report," BlackDuck by Synopsys Center for Open Source Research & Innovation, 2018, https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2018-ossra.pdf.

- communication
- dating
- education
- entertainment
- events
- finance
- food and drink
- games
- health and fitness
- house and home
- libraries and demo
- lifestyle
- maps and navigation
- medical
- music and audio
- news and magazines
- parenting
- personalization
- photography
- productivity
- shopping
- social media
- sports
- tools
- travel and local
- video players
- weather

Given that the goal of the study is to assess the potential risks associated with open source components with known security vulnerabilities that reside within software applications for consumers in the U.S., only applications that are used in the U.S. were selected.

To test for the specific risks associated with the open source components used in the selected applications, Insignary's Clarity tool, a program using fingerprint-based technology to scan binary files in their native format for known and preventable security vulnerabilities, was used.[13] There are several reasons for scanning files in their binary format, as opposed to scanning the source code in its uncompiled programming language:

- Binary files (consisting of ones and zeros) are more easily available for analysis than text-based source code, which companies may view as their proprietary software;
- Binary files are exactly what businesses and consumers receive when they purchase software; and
- Hyper-accurate scanning of binary code is now available, without the need to reverse engineer the software back into its source code – making analyses timely, feasible and cost effective.

These scans provide a potential indicator for the presence of vulnerabilities by comparing the latest known open source components to what is currently in the software. There is one caveat to keep in mind. Because a few firms may elect to customize a patch to reduce vulnerabilities rather than using the latest open source patch, a handful of false positives are possible. This can occur where apps providers "self-patch" their own code, but the scan did not recognize the patch. This study is not able to assess if these solutions fixed the problem or created another one. However, because most applications providers rely exclusively on open-source patches rather than customized solutions – particularly less popular apps which were not considered in this study – the results of these scans are useful indicators of the presence of vulnerabilities.

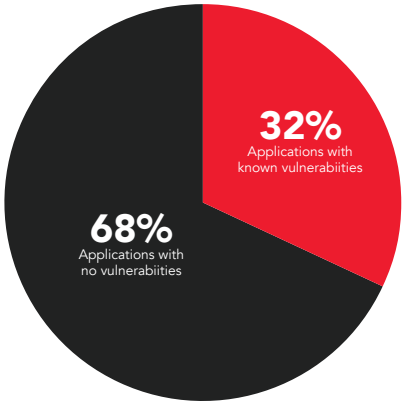
One last thing to keep in mind is that the results in this report represent a onetime snapshot based on the scanned results from the Clarity tool at the time these applications were downloaded and scanned. It is possible that some vulnerabilities were resolved since the applications were originally scanned, or that new vulnerabilities have emerged that were not identified in this report.

13 Binary files were scanned on August 7, 2018 and within weeks of being downloaded in order to minimize the probability of not testing the most updated codebases. For more information about Clarity, see www.insignary.com/get-clarity.

ANALYSIS AND RESULTS

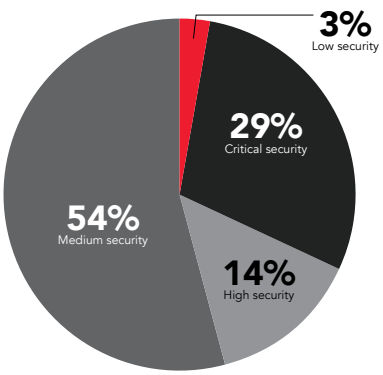
Of the 330 applications that were selected and scanned, 105 of them (32%) were identified to have vulnerabilities (see Figure 1 below) totaling 1,978 vulnerabilities.[14] Based on this, the overall sample averaged 6 vulnerabilities per app (1,978 divided by 330) or an alarming 19 vulnerabilities per app among the 105 identified apps (1,978 divided by 105).

Figure 1: Percentage of Applications with Known Vulnerabilities



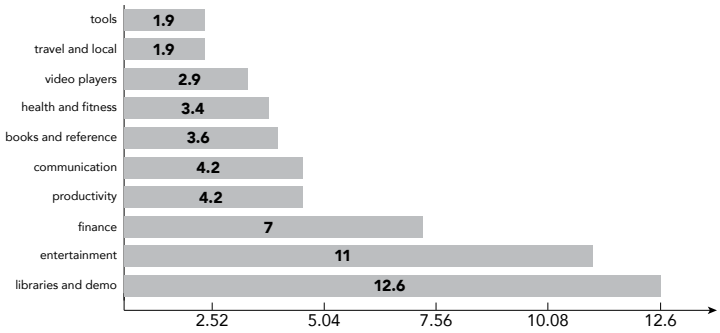
Based on the different scores and associated risks, the National Vulnerability Database ranks each vulnerability as being either a low, medium, high or critical risk, with each designation reflecting an increasing threat. High and critical vulnerabilities are more easily exploited and could cause significantly more damage than low and medium vulnerabilities. Of all the vulnerabilities found in the sample, 43% were considered high risk and critical (see Figure 2).

Figure 2: Distribution of Vulnerabilities Based on Security Risk Severity



Applications in specific categories (e.g., libraries and demo, entertainment, and finance) encountered the most critical vulnerabilities (see Figure 3), suggesting that consumers using applications in these categories may be exposed to major risks and associated damage.[15]

Figure 3: Top 10 Categories with Highest Critical Risk Vulnerabilities per Application



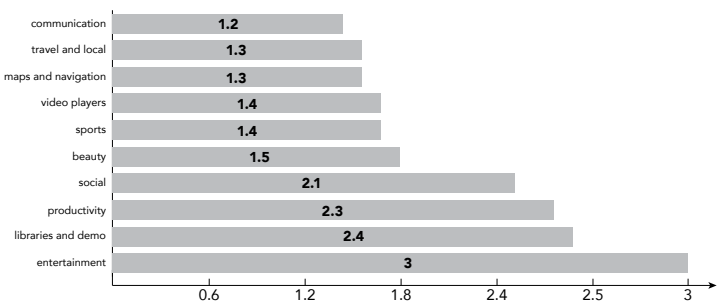
With nearly a third of all major apps containing known and fixable vulnerabilities, the prevalence of risk is widespread. Critical vulnerabilities were found in many common applications, including some of the most popular banking, event ticket purchasing and travel apps, according to the Clarity scan results. For example, Wells Fargo and Bank of America mobile apps each contained over 30 critical vulnerabilities. Other unpatched apps with critical vulnerabilities, according to Clarity's scan, included Sephora, Vivid Seats, TripAdvisor and a wide array of applications that extensively use personal or financial information.

Vulnerabilities categorized as high risk were most frequent in the specific categories of entertainment, libraries and demo, finance, and productivity applications (see Figure 4). High risk vulnerabilities require very little knowledge or skill to exploit, but unlike critical risk vulnerabilities, they will not entirely compromise a device or network system.
The potential damage remains high, as exploited high risk vulnerabilities can partially damage the system and cause information disclosure.

14 Some applications were found to contain the same CVE under different components, so the actual risk probabilities are much higher than reported here.

15 Figure 3 and 4 show vulnerabilities per app for the entire sample of 330. Expressing these ratios relative to just those 105 apps identified as having vulnerabilities would have produced much higher ratios than shown here.

Figure 4: Top 10 Categories with Highest High-Risk Vulnerabilities per Application



Among those identified with high vulnerabilities were some of the best-known sports applications, as well as popular games, dating, social media and fast food apps. Clearly, the presence of these vulnerabilities is a security and privacy problem. This problem, largely unnoticed by general public, appears to be pervasive and could be present on most consumer devices. Yet, these vulnerabilities are preventable with diligent screening and patching.

Overall, the results presented in this study corroborate the findings in other reports (e.g., BlackDuck, Veracode and Insignary) and draw attention to the magnitude of the problem.[16] To make matters even worse, over 40,000 open source vulnerabilities have been reported in the past 17 years, with more than 14,700 new vulnerabilities added to the Common Vulnerabilities and Exposures list in 2017 alone.[17]

At the same time, more companies are now switching to open source code. Take, for example, the London-based Skyscanner Ltd., a travel search engine application that used to run on custom proprietary code, but in recent years has migrated to a wider range of languages and technologies, including open source.[18] Skyscanner is not alone.[19] State and local governments are joining the trend and jumping onto open source for its ability to save software development time and overall costs. In other words, open source is growing and is here to stay, which makes business and consumer users potentially valuable targets for hackers.

Unfortunately, we do not live in an ideal world where applications update themselves the instant a security fix becomes available without any intervention required. Until that becomes possible, more due diligence by software vendors, their third-party software developers, and software security management consultants appears to be a solid first line of defense in finding software components that harbor known security vulnerabilities. This will reduce the possibility of damage inflicted on both companies and their customers by hackers. The 2017 Veracode report shows that simply putting an application testing program in place can help an organization start chipping away at its flaws.[20]

16 For references to these studies, see "The State of Software Security 2017, " Veracode, CA Technologies, 2017, and see footnotes 3 and 4 of this study.

17 See the Common Vulnerabilities and Exposures database at https://cve.mitre.org.

18 Maria Korolov, "Open source software security challenges persist," CSO, IDG Communications, April 2, 2018, https://www.csoonline.com/article/3157377/application-development/open-source-software-security-challenges-persist.html.

19 Dharmesh Thakker, Max Schireson and Dan Nguyen-Huu, "Tracking the explosive growth of open-source software." TechCrunch, April 7, 2017, https://techcrunch.com/2017/04/07/tracking-the-explosive-growth-of-open-source-software/.

20 "The State of Software Security 2017," Veracode, CA Technologies, 2017.

SUMMARY TABLE: POTENTIAL VULNERABILITIES PER APPLICATION SAMPLED

Category	Total	Critical	High	Medium	Low
Entertainment	1.9	0.1	0.6	1.2	0.0
Libraries and demo	0.6	0.0	0.0	0.6	0.0
Finance	6.8	0.7	1.5	4.4	0.2
Books and reference	8.1	3.6	0.3	4.0	0.2
Social	1.4	0.1	0.5	0.8	0.0
Productivity	2.9	0.2	0.3	2.3	0.1
Travel and local	10.3	4.2	1.2	4.8	0.1
Communication	5.1	0.2	1.0	3.6	0.3
Video player	2.3	0.1	0.3	1.9	0.0
Dating	29.5	11.0	3.0	15.0	0.5
Sports	3.8	1.9	0.5	1.4	0.0
Food and drink	13.0	7.0	0.9	4.9	0.2
Health and fitness	5.0	0.0	1.0	3.9	0.1
Music and audio	1.9	0.0	0.5	1.4	0.0
Beauty	7.0	3.4	0.7	2.8	0.1
Comics	2.2	0.0	0.4	1.6	0.2
Maps and navigation	25.0	12.6	2.4	10.0	0.0
Photography	0.5	0.0	0.0	0.5	0.0
Tools	4.7	0.0	1.3	3.2	0.2
Events	0.3	0.0	0.0	0.3	0.0
Education	3.1	0.4	1.0	1.7	0.0
House and home	2.1	0.0	0.5	1.5	0.1
Art and design	0.2	0.0	0.0	0.2	0.0
News and magazines	0.3	0.0	0.2	0.1	0.0
Games	3.3	0.5	0.5	2.2	0.1
Auto and vehicles	14.3	4.2	2.3	7.3	0.5
Business	0.4	0.0	0.3	0.1	0.0
Lifestyle	11.8	1.2	2.1	7.9	0.6
Medical	6.0	0.1	1.4	4.3	0.2
Shopping	4.4	1.9	0.6	1.9	0.0
Personalization	9.1	1.9	1.3	5.6	0.3
Weather	10.2	2.9	1.4	5.4	0.5
Parenting	0.3	0.0	0.1	0.2	0.0

RETESTING: APPS WITH CRITICAL VULNERABILITIES

Among the many apps that tested positive for known online risks, Wells Fargo and Bank of America both encountered the highest frequency of critical vulnerabilities in the finance category – each with over 30 critical vulnerabilities – according to Insignary's Clarity scanning software. For example, both banking apps were found to include CVE-2013-0749, a vulnerability with critical risks that could allow attackers remote access to devices that could crash the application or lead to denial of service attacks or memory corruption.

Several weeks following our initial scans, we retested the new binary codes for the Wells Fargo and Bank of America apps and found both had patched their software for all the vulnerabilities found in the previous versions. Yet, we note the critical importance of shrinking the window of time that attackers can use to their advantage to target specific vulnerabilities. Patching software can be costly and takes time, as it is a complex process that involves first identifying the vulnerabilities, then implementing and testing the patches before they are made public. Given the magnitude of risks associated with potential attacks, businesses should prioritize working on solutions that reduce the vulnerable time frame.

On the other hand, we also checked several apps and found nothing had changed—fixable vulnerabilities had not been addressed. For example, one popular app used as a platform to buy and sell event tickets, Vivid Seats, had the highest risk in its category, including 19 critical vulnerabilities. After retesting the newest software, the Clarity scans showed that the Vivid Seats software was still suffering from the same vulnerabilities.

What our snapshot analysis showed is the widespread prevalence of known and patchable vulnerabilities. While some companies may have the resources to create patches and some may update their applications from time to time, there are often delays that provide a window of opportunity for hackers to do harm. For other firms, particularly those with limited means, modest budgets or lack of awareness, these risks may seldom be mitigated, leaving vulnerabilities that expose companies and consumers to potential security and privacy breaches. While the magnitude and types of risk heavily depend on the type of business (i.e. finance apps will probably store more sensitive information than fitness apps), the security and data privacy of consumers should be a concern to all.

FURTHER IMPLICATIONS OF VULNERABILITIES IN OPEN SOURCE SOFTWARE

Software has become ubiquitous in our daily lives, directing the devices and applications that are key to modern commerce, the digital economy, and our critical infrastructure. Yet, despite the promising and necessary growth in applications, cyberattacks are more far-reaching and consequential than we could have imagined just a few years ago. Data breaches are on the rise in businesses across different sectors of the economy, becoming a real danger for both brands and their customers.[21]

As new technologies are developed, open source security will become more challenging. Mitigating security vulnerabilities in autonomous vehicles and medical devices will be an especially difficult task. Open source components are widely used in virtually all forms of open and proprietary applications. Automobile manufacturers, for example, rely on a wide range of component and application suppliers who build software with open source components and extend open source platforms.

Not too long ago, it was discovered that some of Tesla's automotive infotainment systems contained a four-year-old vulnerability that could potentially let an attacker conduct a fully remote hack to start the car or cut the motor.[22] This is not an isolated example in the automotive industry and containing these risks will become more challenging as open source code is channeled through countless supply chains in almost every part of the automotive industry.

21 Dennis Green, "If You Shopped at These 15 Stores in the Last Year, Your Data Might Have Been Stolen," Business Insider, July 1, 2018, https://read.bi/2q2ryJ0.

22 "2018 Open Source Security and Risk Analysis Report," BlackDuck by Synopsys Center for Open Source Research & Innovation, 2018, https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2018-ossra.pdf.

Medical devices are yet another prime example of the rapidly increasing challenge posed by hackers targeting open source vulnerabilities. On December 28, 2016, the U.S. Food and Drug Administration (FDA) finalized its guidance on the "Postmarket Management of Cybersecurity in Medical Devices."[23] The guidance highlighted a real and often overlooked source of security vulnerabilities that can be easily exploited, potentially leading to physical harm or even death to patients. The key challenge, as in the automotive industry, is with third-party components that are difficult to monitor. With the surge of IoT applications and interconnected equipment, the presence of unsupported electronic devices will provide a growing target for hackers for years to come.

Software is arguably the key driver of the technological innovation happening across a spectrum of industries that includes medical devices, automobile manufacturing, baby monitors and the Internet of Things, among many others. And, that software is primarily built on a core of open source code.

We believe that Google App Store apps are a suitable proxy for all enterprise, consumer and embedded software that utilizes open source components. As this study shows, application developers need to invest the resources and institute processes for finding known security vulnerabilities in their code and patching them. This is a logical, first step in a more comprehensive effort needed to protect consumers and businesses from hackers. Before government regulators intervene, application developers should take immediate, proactive steps to patch their applications that contain open source components and notify consumers when software updates are available. The potential for serious damage will only increase as open source code becomes even more widely used. The time to act is now.

In summary, this study has explored the degree to which some applications and software code are being left unpatched for known risks, making them more susceptible to cybercrime and other online threats. It is imperative that apps providers address these known security flaws to prevent consumer devices from being compromised and to protect the public against malicious online activity, loss of personal and company information, and identity theft. Apps providers need to develop best-practices now that will reduce these risks, or it will likely face a backlash from the public and policymakers.

23 "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," U.S. Department of Health and Human Services, U.S. Food and Drug Administration, December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Appendix

SAMPLE OF APPS IN THE STUDY

Application Name	Category
2018 FIFA WORLD CUP	SPORTS
360 SECURITY	TOOLS
365SCORES	SPORTS
8 BALL POOL	GAMES
ACCUWEATHER	WEATHER
ADA YOU HEALTH GUIDE	MEDICAL
ADOBE ACROBAT READER	PRODUCTIVITY
AKINATOR	ENTERTAINMENT
ALARMY	LIFESTYLE
ALFRED HOME SECURITY	HOUSE AND HOME
ALIEXPRESS	SHOPPING
AMAZON KINDLE	BOOKS AND REFERENCE
AMAZON SHOPPING	SHOPPING
ANATOMY LEARNING 3D	MEDICAL
ANDROID AUTO MAPS	AUTO AND VEHICLES
ANIMESKINS	EVENTS
APUS LAUNCHER	PERSONALIZATION
AUDIOBOOKS	BOOKS AND REFERENCE
AUTO TRADER	AUTO AND VEHICLES
AUTOSCOUT24	AUTO AND VEHICLES
AVAST MOBILE	TOOLS
AVG ANTIVIRUS	TOOLS
AVIARY EFFECTS	LIBRARIES AND DEMO
AVIARY STICKERS	LIBRARIES AND DEMO
B612 BEAUTY FILTER	PHOTOGRAPHY
BABBEL	EDUCATION
BABY SLEEP	PARENTING
BACKGROUNDS HD	PERSONALIZATION
BADOO	SOCIAL
BATTERY DOCTOR	TOOLS
BEAUTY CAMERA	BEAUTY
BBC NEWS	NEWS AND MAGAZINES

Application Name	Category
BEAUTY MAKEUP	BEAUTY
BEAUTYLISH	BEAUTY
BEAUTYPLUS	PHOTOGRAPHY
BEST HAIRSTYLES	BEAUTY
BIBLE DAILY	BOOKS AND REFERENCE
BIBLE OFFLINE	BOOKS AND REFERENCE
BITMOJI	ENTERTAINMENT
BOFA	FINANCE
BOOKING.COM	TRAVEL AND LOCAL
BRAINLY	EDUCATION
CALL BLOCKER	BUSINESS
CALORIE COUNTER	HEALTH AND FITNESS
CAMERA 360	PHOTOGRAPHY
CANDY CAMERA	PHOTOGRAPHY
CANDY CRUSH	GAMES
CANVA POSTER	ART AND DESIGN
CARDBOARD	LIBRARIES AND DEMO
CARS.COM	AUTO AND VEHICLES
CHASE ANDROID	FINANCE
CLASH OF CLANS	GAMES
CLASH ROYALE	GAMES
CLEAN MASTER SPACE	TOOLS
CM LAUNCHER 3D	PERSONALIZATION
COLORNOTE	PRODUCTIVITY
COMPASS	MAPS AND NAVIGATION
COOCKPAD	FOOD AND DRINK
CREDITKARMA	FINANCE
CTNCARDOSO	AUTO AND VEHICLES
DAILY ROADS	AUTO AND VEHICLES
DAILYHUNT NEWSHUNT	NEWS AND MAGAZINES
DATA RECHARGE	LIFESTYLE
DAYS LEFT COUNTDOWN	EVENTS
DEEZER	MUSIC AND AUDIO
DIARY WITH LOCK	LIFESTYLE
DICTIONARY.COM	BOOKS AND REFERENCE
DOGETHER	EVENTS

Application Name	Category
DOMINO'S ONLINE	FOOD AND DRINK
DOMINO'S USA	FOOD AND DRINK
DRAW CARTOONS	COMICS
DREAM LEAGUE	GAMES
DROPBOX	PRODUCTIVITY
DUBSMASH	VIDEO PLAYER
DUOLINGO	EDUCATION
EBAY	SHOPPING
EDOMETER	HEALTH AND FITNESS
ELEVATE BRAIN TRAINING	EDUCATION
ENDOMONDO RUNNING	HEALTH AND FITNESS
ES FILE EXPLORER	PRODUCTIVITY
ESPN	SPORTS
EYEWIND PAPERONE	ART AND DESIGN
FACEBOOK LITE	SOCIAL
FACEBOOK PAGES	BUSINESS
FACEBOOK PAGES	SOCIAL
FAMILY ALBUM MITENE	PARENTING
FAMILY LOCATOR GPS	LIFESTYLE
FAMILY LOCATOR GPS TRACKER V4	PARENTING
FEED BABY	PARENTING
FEEDLY	NEWS AND MAGAZINES
FEVER	EVENTS
FILE COMMANDER	BUSINESS
FIND REAL LOVE	DATING
FLIPACLIP	ART AND DESIGN
FLIPBOARD NEWS	NEWS AND MAGAZINES
FOLLOW MY HEALTH	MEDICAL
FOODPANDA	FOOD AND DRINK
FOTMOB WORLD CUP	SPORTS
FOURSQUARE	FOOD AND DRINK
FREE DATING APP	DATING
FREE GPS NAVIGATION	MAPS AND NAVIGATION
FUELIO	AUTO AND VEHICLES
GALAXY CHAT	DATING
GAMETIME	EVENTS

Application Name	Category
GASBUDDY	TRAVEL AND LOCAL
GEEK SMARTER SHOPPING	SHOPPING
GEOZILLA GPS LOCATOR	PARENTING
GO KEYBOARD	PERSONALIZATION
GO LAUNCHER 3D	PERSONALIZATION
GO WEATHER WIDGET	WEATHER
GOOGLE	SOCIAL
GOOGLE CHROME	COMMUNICATION
GOOGLE DRIVE	PRODUCTIVITY
GOOGLE EARTH	TRAVEL AND LOCAL
GOOGLE NEWS	NEWS AND MAGAZINES
GOOGLE PAY	FINANCE
GOOGLE PHOTOS	PHOTOGRAPHY
GOOGLE PLAY BOOKS	BOOKS AND REFERENCE
GOOGLE PLAY GAMES	ENTERTAINMENT
GOOGLE PLAY MUSIC	MUSIC AND AUDIO
GOOGLE PLAY SERVICES	TOOLS
GOOGLE STREET VIEW	TRAVEL AND LOCAL
GOOGLE TRANSLATE	TOOLS
GOOGLE V8	TOOLS
GRABTAXI DRIVER	MAPS AND NAVIGATION
GRABTAXI PASSENGER	MAPS AND NAVIGATION
GROUPON	SHOPPING
GRUBHUB	FOOD AND DRINK
HAPPN	LIFESTYLE
HAY DAY	GAMES
HERE WEGO	MAPS AND NAVIGATION
HILL CLIMB RACING	GAMES
HITWE	DATING
HOT OR NOT	DATING
HOUZZ	HOUSE AND HOME
HTC	LIBRARIES AND DEMO
HWAHAE	BEAUTY
I'M PREGNANT	PARENTING
IBIS PAINT	ART AND DESIGN
IHEARTRADIO	MUSIC AND AUDIO

Application Name	Category
INDEED JOB	BUSINESS
INSTAGRAM	SOCIAL
IPAIR	DATING
IPSY	BEAUTY
IQOPTION	FINANCE
JOOM	SHOPPING
JW LIBRARY	BOOKS AND REFERENCE
KIKA KEYBOARD	PRODUCTIVITY
KONYLABS	FINANCE
LADYTIMER	MEDICAL
LEARN TO DRAW ANIME	COMICS
LETGO	SHOPPING
LINE FREE CALLS	COMMUNICATION
LINE WEBTOON	COMICS
LINKEDIN JOB SEASRCH	BUSINESS
LINKEDIN SLIDESHARE	BUSINESS
LIVESCORE	SPORTS
MAKEMYTRIP	TRAVEL AND LOCAL
MANGA ROCK	COMICS
MAPFACTOR	MAPS AND NAVIGATION
MAPS GPS NAVIGATION	MAPS AND NAVIGATION
MAPS ME	TRAVEL AND LOCAL
MAPS NAVIGATION	TRAVEL AND LOCAL
MARVEL COMICS	COMICS
MATH TRICKS	EDUCATION
MCDONALDS	FOOD AND DRINK
MEDIBANG	ART AND DESIGN
MEMRISE	EDUCATION
MESSENGER TEXT	COMMUNICATION
METAQUOTES	FINANCE
MICROSOFT OUTLOOK	PRODUCTIVITY
MICROSOFT WORD	PRODUCTIVITY
MIRROR ZOOM	BEAUTY
MOCO CHAT	DATING
MOM LIFE	PARENTING
MOOVIT	MAPS AND NAVIGATION

Application Name	Category
MPR VIDEO CONVERTER	MUSIC AND AUDIO
MUSICAL.LY	SOCIAL
MUSLIM PRO RAMADAN	LIFESTYLE
MX PLAYER CODEC ARM V5	LIBRARIES AND DEMO
MX PLAYER CODEC ARM V6	LIBRARIES AND DEMO
MX PLAYER CODEC ARM V6 VFP	LIBRARIES AND DEMO
MX PLAYER CODEC ARM V7	LIBRARIES AND DEMO
MX PLAYER CODEC ARM V7 NEON	LIBRARIES AND DEMO
MX PLAYER CODEC TEGRA3	LIBRARIES AND DEMO
MX PLAYER V1	VIDEO PLAYER
MY CALENDAR PERIOD	MEDICAL
NARATOR'S VOICE	COMICS
NAVER	COMICS
NETFLIX	ENTERTAINMENT
NEURONATION	EDUCATION
NEWS REPUBLIC	NEWS AND MAGAZINES
NFL	SPORTS
NIKE RUN CLUB	HEALTH AND FITNESS
OFFICESUITE	BUSINESS
OKCUPID	DATING
ONCE QUALITY	DATING
ONEFOOTBALL WORLD CUP	SPORTS
OPERA MINI	COMMUNICATION
OVIA PREGNANCY TRACKER	MEDICAL
PANDORA	MUSIC AND AUDIO
PARALLEL SPACE	PERSONALIZATION
PAYPAL	FINANCE
PEAK BRAIN GAMES	EDUCATION
PEEKABOO	PARENTING
PEEL UNIVERSAL SMART	HOUSE AND HOME
PERFECT VIEWER	COMICS
PERIOD AND OVULATION	MEDICAL
PERIOD TRACKER CLUE	HEALTH AND FITNESS
PERIOD TRACKER FLO	HEALTH AND FITNESS
PERIOD TRACKER PERIOD	HEALTH AND FITNESS
PERIOD TRACKER V1	MEDICAL

Application Name	Category
PHOTOGRID	PHOTOGRAPHY
PHOTOMATH	EDUCATION
PICSART	PHOTOGRAPHY
PINTEREST	SOCIAL
PODCAST ADDICT	NEWS AND MAGAZINES
POKEMON GO	GAMES
PREGNANCY	MEDICAL
PREGNANCY TRACKER	PARENTING
PREGNANCY WEEK BY WEEK	MEDICAL
PRIVATE ZONE APPLOCK	VIDEO PLAYER
RAGE COMIC MAKER	COMICS
REAL ESTATE HOUSES	HOUSE AND HOME
REALTOR.COM	HOUSE AND HOME
REDDIT IS FUN	NEWS AND MAGAZINES
REDDIT TOP NEWS	NEWS AND MAGAZINES
REMINDER	EVENTS
RETRICA	PHOTOGRAPHY
ROOM CREATOR	HOUSE AND HOME
RUNKEEPER	HEALTH AND FITNESS
RUNTASTIC	HEALTH AND FITNESS
SAMSUNG PAY	LIFESTYLE
SAND DRAW SKETCH	ART AND DESIGN
SEATGEEK	EVENTS
SECURITY MASTER	TOOLS
SEPHORA	BEAUTY
SEX OFFENDER SEARCH	PARENTING
SHADOW FIGHT 2	GAMES
SHAREIT	TOOLS
SHAZAM	MUSIC AND AUDIO
SING BY SMULE	MUSIC AND AUDIO
SKETCH DRAW PAINT	ART AND DESIGN
SKY MAP	BOOKS AND REFERENCE
SKYPE	COMMUNICATION
SNAPCHAT	SOCIAL
SNAPDEAL	SHOPPING
SOFASCORE	SPORTS

Application Name	Category
SOLO LAUNCHER	PERSONALIZATION
SOUNDCLOUD	MUSIC AND AUDIO
SPEEDOMETERS	AUTO AND VEHICLES
SPOTIFY	MUSIC AND AUDIO
STARBUCKS	LIFESTYLE
STUBHUB	EVENTS
SUBWAY SURFERS	GAMES
SUPER BRIGHT LED	PRODUCTIVITY
SURE UNIVERSAL	HOUSE AND HOME
SWIFT WIFI FREE	TRAVEL AND LOCAL
SWIFTKEY	PRODUCTIVITY
SWIGGY	FOOD AND DRINK
TALKING ANGELA	ENTERTAINMENT
TALKING BEN THE DOG	ENTERTAINMENT
TALKING GINGER	ENTERTAINMENT
TALKING TOM CAT	ENTERTAINMENT
TALKING TOM CAT 2	ENTERTAINMENT
TANGO LIVE	SOCIAL
TASTELY	LIFESTYLE
TEXTART	ART AND DESIGN
TEXTGRAM	ART AND DESIGN
THE AVENGERS	COMICS
THE WEATHER V2	WEATHER
THE WEATHER CHANNEL	WEATHER
TICKETMASTER	EVENTS
TIK TOK	VIDEO PLAYER
TINDER	LIFESTYLE
TINY SCANNER	BUSINESS
TINYCAM	HOUSE AND HOME
TOCA KITCHEN	EDUCATION
TRANSPARENT CLOCK WEATHER	WEATHER
TRIPADVISOR	TRAVEL AND LOCAL
TRUECALLER	COMMUNICATION
TRUEMONEY WALLET	FINANCE
TRULIA REAL ESTATE	HOUSE AND HOME
TRULIA RENT	HOUSE AND HOME

Application Name	Category
TUMBLR	SOCIAL
TUNEIN STREAM NFL	MUSIC AND AUDIO
TWITCH	ENTERTAINMENT
TWITTER	NEWS AND MAGAZINES
U LAUNCHER LITE	ART AND DESIGN
UBER	MAPS AND NAVIGATION
UBER EATS	FOOD AND DRINK
UBERCAB DRIVER	BUSINESS
UC BROWSER	COMMUNICATION
ULTA BEAUTY	BEAUTY
ULYSSE SPEEDOMETER	AUTO AND VEHICLES
USED CARS FOR SALE	AUTO AND VEHICLES
VAULT HIDE	BUSINESS
VIBER	COMMUNICATION
VIDEO EDITOR	PHOTOGRAPHY
VIDEO SHOW	VIDEO PLAYER
VIGO VIDEO	VIDEO PLAYER
VINE	VIDEO PLAYER
VIVAVIDEO	VIDEO PLAYER
VIVID SEATS	EVENTS
VLC	VIDEO PLAYER
WATCH ESPN	SPORTS
WATER DRINK REMINDER	HEALTH AND FITNESS
WATTPAD	BOOKS AND REFERENCE
WAZE	MAPS AND NAVIGATION
WEATHE LIVE	WEATHER
WEATHER	WEATHER
WEATHER BY WEATHERBUG	WEATHER
WEATHER CLOCK WIDGET	WEATHER
WECHAT	COMMUNICATION
WELLS FARGO MOBILE	FINANCE
WHAFF	SHOPPING
WHATSAPP	COMMUNICATION
WHATSAPP WALLPAPER	PERSONALIZATION
WIFI MAP	TRAVEL AND LOCAL
WIKIPEDIA	BOOKS AND REFERENCE

Application Name	Category
WISH SHOPPING	SHOPPING
YAHOO FANTASY SPORTS	SPORTS
YAHOO WEATHER	WEATHER
YOUCAM	BEAUTY
YOUCAM MAKEUP	PHOTOGRAPHY
YOUTUBE	VIDEO PLAYER
ZEDGE	PERSONALIZATION
ZERO LAUNCHER	PERSONALIZATION
ZOMATO	FOOD AND DRINK
ZOOSK	DATING