BITSIGHT®
The Standard in SECURITY RATINGS

BitSight Insights

Mobile Application
Risk Report

Contents

BitSight Performance Analysis Identifies Significant Gaps in Mobile Application Security Initiatives Across Sectors

As security and risk professionals take steps to improve their organization's cybersecurity posture, email, network, and web security often take center stage. This makes perfect sense, as these have been preferred attack vectors for decades. However, as internet use continues to move toward a mobile-centric experience, it has become critical to consider mobile applications when crafting your organization's security strategy.

In this report, you'll find eye-opening statistics on the state of mobile application security today, examples of how and why mobile breaches occur, and actionable advice for mitigating risks associated with your own mobile applications, as well as apps from third-party partners and suppliers.

You'll also get BitSight's latest research on mobile application security—including performance stats by application genre, sector, and popularity. Finally, you'll learn how to reduce risk and demonstrate security performance to customers, prospects, and other critical stakeholders.

Key Research Findings

01 3 out of 4 mobile applications evaluated contained at least one Moderate vulnerability. The prevalence of at least one Material (<1%) or Severe (2.5%) vulnerability occurs at significantly lesser rates.

02 Material and Severe vulnerabilities, including Arbitrary Code Execution, were observed in highly popular mobile apps.

03 Very few Material and Severe vulnerabilities were remediated once they were in production. Remediation rates were very low given the criticality of these vulnerabilities.

04 Android shopping apps, which transmit personal identifying information (PII) and other sensitive financial details, performed poorly in TLS Certificate Validation for Sensitive Data.

05 GPS Data Leakage, a significant security and privacy issue, was a problem across a variety of sectors and mobile app genres—including Aerospace and Defense.

The Increasing Risk to Mobile Applications

Since mobile applications store massive amounts of users' personal information, breaches and data leakage can expose organizations to significant risk, as evidenced by news coverage throughout 2021.

In March, a breach in its mobile app forced a Formula 1 racing team to call off an augmented reality campaign after its app was hacked. In June, a healthcare provider was breached via unauthorized access to a third-party mobile app called Smart Clinic.

In August, British Airways disclosed that approximately 380,000 card payments were compromised after a security breach occurred on the company's website and mobile app. The breach compromised the personal and financial details of customers—including name, address, and bank card details like CVC code.

In September, security researchers found that 14 top Android apps, downloaded by more than 140 million people in total, are leaking user data due to Firebase misconfigurations. Exposed data potentially includes users' names, emails, usernames, and other PII. Firebase is a mobile application development platform with an active monthly base of more than 2.5 million apps.

"Mobile applications already drive much of today's digital activity and that will only increase in the future. 5G, increased work-from-home, and the ever-increasing availability of mobile devices have all but assured that cyber criminals will look for avenues into mobile applications to conduct attacks," said Stephen Boyer, Founder and CTO of BitSight. "For these reasons, it is critical for organizations to understand risks associated with mobile applications created in-house and those published by third parties."

"It is critical for organizations to understand risks associated with mobile applications created in-house and those published by third parties."

- STEPHEN BOYER
Founder and CTO of BitSight

BitSight's Evaluation of Mobile Application Security Performance

There are [approximately 5 million mobile apps currently in circulation](#): approximately 3 million for Android and 2 million for iOS. Of the millions of mobile apps available, a significantly smaller subset dominates the market. Of these, only a small proportion constitutes the mainstream mobile apps.

BitSight wanted to understand the prevalence of vulnerabilities in popular mobile applications across a variety of sectors and industries. We analyzed 93,647 mobile apps from 40,664 organizations and tasked ourselves with answering two critical questions:

1. How common are significant vulnerabilities in mobile applications?
2. Are some sectors better or worse than others in addressing mobile application security issues?

In our analysis, we analyzed 185 static and dynamic mobile application tests that investigated all vulnerability types—from Minor to Severe—across 22 major industry sectors.

BitSight Methodology: Severity Levels and Mobile Application Grades

Before we dive into the results of our research, it is important to understand how BitSight uses the [Common Vulnerability Scoring System (CVSS)](#). CVSS is a widely-used evaluation of the magnitude of vulnerabilities on a ten-point scale. However, BitSight uses different nomenclature than CVSS to retain consistency with existing notions of severity within BitSight's platform.

CVSS RANGE	BITSIGHT SEVERITY	CVSS RANGE
0.0	Minor	Informational
0.1 - 3.9	Minor	Low
4.0 - 6.9	Moderate	Medium
7.0 - 8.9	Material	High
9.0 - 10.0	Severe	Critical

BitSight leverages mobile application vulnerabilities to create an overall [Mobile Application Security grade](#) of an organization's published applications. The BitSight Mobile Application Security grade is a value between 0 to 10, derived from the CVSS scores of vulnerabilities detected, such that: (1) the app grade is greater than or equal to the largest CVSS score of the detected vulnerabilities, and (2) each detected vulnerability with a positive CVSS score worsens (i.e. increases) the app grade. The lower the grade, the more secure the application. A detailed methodology of BitSight's approach is available within the [BitSight Knowledge Base](#).

Vulnerability Severity Prevalence in Mobile Apps

BitSight examined vulnerability severity prevalence across mobile applications in all sectors. For each specific vulnerability, we considered the results of either a static or a dynamic analysis test and defined test failure rate as the probability that an app will fail at least one test at a given vulnerability level. We also aggregated data across multiple security flaws into their respective CVSS severities for brevity.

> BitSight's analysis showed that Minor and Moderate test failures were far more common than Material and Severe test failures.
>
> The probability of observing a Severe vulnerability in a mobile app was less than one percent. Observing a Material vulnerability was only slightly more probable (**2.5%**). Moderate vulnerabilities were far more common with a probability of **74.7%** and Minor vulnerabilities were **59.2%** probable.

As the following sections describe, Material and Severe vulnerabilities were observed in some highly popular mobile apps. Worse, very few Material and Severe vulnerabilities were remediated once they were in production.

Finally, it is important to note that even Minor and Moderate vulnerabilities can expose organizations to serious risks. For example, short encryption keys are classified as Moderate, but they can leave apps vulnerable to brute force attacks. In our study, this type of vulnerability was fairly common. We found insufficient signing key length present in roughly a quarter of the Android apps analyzed.

Overall Mobile Application Security Performance By Sector Over 12 Months

Leveraging mobile application security testing data, we ranked sectors in terms of their average mobile application security performance over a twelve month period.

Finance, Insurance, and Retail came in on top of this list while Nonprofit/NGO, Business Services, and Media/Entertainment performed poorly by comparison.

However, the average BitSight application scores were quite close across sectors—ranging from 5.36 and 6.04. The reality is that a typical mobile app release is shipped to the end-user with a strong likelihood of containing a Minor or Moderate vulnerability, regardless of sector.

Rank	Sector	Average BitSight AppSec Grade	Unique App Count	Percentage of Apps with 1+ Test Failure(s)		
				Minor	Moderate	Material + Severe
1	Finance	5.36	9898	53	57	2
2	Insurance	5.51	1791	57	65	2
3	Retail	5.54	2175	52	67	3
4	Transportation	5.56	2315	55	69	3
5	Food Production	5.58	781	54	71	2
6	Government/Politics	5.61	2869	55	81	2
7	Engineering	5.63	980	61	81	2
8	Manufacturing	5.67	2804	54	77	3
8	Consumer Goods	5.67	1447	53	75	4
8	Energy/Resources	5.67	1004	61	76	3
8	Utilities	5.67	587	59	75	1
12	Legal	5.69	146	64	81	4
13	Tourism/Hospitality	5.73	2508	56	78	3
13	Telecommunications	5.73	3272	56	72	3
15	Aerospace/Defense	5.74	224	55	73	4
16	Technology	5.77	41029	63	78	2
17	Real Estate	5.81	641	53	74	4
18	Education	5.82	3510	58	82	4
19	Healthcare/Wellness	5.83	5647	70	81	1
20	Nonprofit/NGO	5.94	1178	68	83	2
21	Business Services	6.03	6191	61	80	4
22	Media/Entertainment	6.04	8242	64	83	6

Material and Severe Vulnerability Prevalence By Sector

BitSight examined how specific sectors performed on Material and Severe vulnerabilities to identify areas of high and low performance. Overall, sectors performed well on the majority of tests. However, we identified some concerning trends.

For example, we observed Leakage of Location (GPS + ZIP Code) via HTTP for both iOS and Android apps and Leakage of PII (e-mail address, first/last names) via HTTP in iOS apps in the Aerospace/Defense sector. Data leakage of this type could have serious ramifications—especially in Aerospace/Defense where compromise may have national security implications.

Additional findings included:

- Improper TLS Certificate Validation for Sensitive Data in the Retail, Technology, Tourism/Hospitality, and Transportation sectors.

- Leakage of Apple AdID via HTTP in iOS apps in the Media/Entertainment and Business Services sectors.

Apple AdID, or Advertising Identifier, is an alphanumeric string used specifically for advertising that uniquely identifies a specific device to the app's vendor. AdID leaks have potential privacy, compliance, and security implications.

For more detail, see Heatmaps 1 and 2 in the appendix.

Material and Severe Vulnerability Percentage by App Genre

Next, we investigated Material and Severe vulnerability prevalence by Android and iOS app store genre. In this round, we limited our testing to popular app genres—which we defined as genres that include over 1,000 apps.

Overall, we found that issues with TLS Certificate Validation for Sensitive Data are prevalent across many genres of Android apps. Shopping apps, which transmit PII and other sensitive financial details, performed worst in this area.

Improper TLS Certificate Validation for Sensitive Data is a concern across almost all genres of iOS apps. News apps are the most problematic genre for iOS.

Additional findings included:

- Android apps for News are the most likely to be vulnerable to Arbitrary Code Execution.

- GPS tracking data (latitude + longitude) leaked via HTTP can be a serious problem for some social apps on Android.

- Leakage of Apple AdID via HTTP in iOS news apps is much more prevalent than for other genres.

- Leakage of PII (first name) and Apple IDFV via HTTP was also observed.

Apple IDFV, or Identifier For Vendor, is an alphanumeric string that uniquely identifies a specific device to the app's vendor. IDFV leaks have potential privacy, compliance, and security implications.

For more detail, see Heatmaps 3 and 4 in the appendix.

Material and Severe Vulnerability Percentage by App Popularity

We also wanted to better understand how common serious vulnerabilities are among the most popular mobile applications. We investigated Material and Severe vulnerability prevalence by user engagement (download counts, app ratings).

Some highly popular mobile apps were observed to have Material and Severe vulnerabilities. For example, nearly all the Android apps we found to be susceptible to Arbitrary Code Execution are very popular (more than 1,000,000 downloads). Improper TLS Certification is prevalent in iOS apps with user download counts ranging from 1,000 to 10,000.

Additional findings included:

- Improper TLS Certificate Validation for Sensitive data occurs in some popular Android apps.
- Leakage of GPS Coordinates via HTTP can be an issue for some popular Android apps.
- Leakage of Apple AdID via HTTP was observed for some iOS apps with a wide range of user-engagement levels (100 to 100,000 downloads)

For more detail, see Heatmaps 5 and 6 in the appendix.

Material and Severe Vulnerability Remediation By Sector

We examined Material and Severe remediation rates by sector. A mobile app was deemed to have undergone remediation if:

- The latest available version was tested to be insusceptible to a given vulnerability, and
- The vulnerability was observed in an earlier version(s) tested in the last year.

Overall, very few Material and Severe vulnerabilities were remediated once they were in production. The remediation rates that BitSight observed were very low given the criticality of these vulnerabilities.

On a positive note, we found that iOS apps in the Media/Entertainment sector have high remediation rates for Apple IDFV Leakage via HTTP. In fact, test results in this category were better than any other sector/vulnerability. The Insurance and Transportation sectors also performed well in this area.

Additional findings included:

- Android Real Estate apps had the highest remediation rates for GPS data leakage via HTTP.
- Some iOS Tourism/Hospitality apps performed well in the PII (last name) Leakage via HTTP remediation while others did not.
- TLS Certificate Validation Issues for Sensitive Data on iOS in Energy/Resources, Telecommunications, and Transportation apps were observed to have been remediated in some cases.

For more detail, see Heatmaps 7 and 8 in the appendix.

Improving Mobile Application Security

When evaluating mobile applications security, organizations must consider their own apps as well as those published by third parties. It is essential that organizations enforce security standards as an essential part of their mobile app development and release cycles.

Mobile app security evaluations should not be treated as the last step of the development and/or release process, but as recurring functionality milestones. All apps—not just a select few—should be included in the security evaluation process. Additionally, mobile applications should be evaluated on an ongoing basis.

"We believe that developers of mobile apps in lower performing sectors are likely laser-focused on the features and functionalities of their products. Additionally, security evaluations may often occur after apps have been developed by teams whose core expertise is not in security," said Abdullah Al Rashid, Senior Data Scientist at BitSight. "It is a worthwhile investment for organizations to continuously vet apps for security issues to reduce risk."

> "It is a worthwhile investment for organizations to continuously vet apps for security issues to reduce risk."
>
> **- ABDULLAH AL RASHID**
> *Senior Data Scientist at BitSight*

Vetting mobile application security can be challenging, but thankfully there are tools that can help. BitSight's Mobile Application Security (Mobile AppSec) rating distills results from static and dynamic analysis of apps into intuitive letter grades, enabling organizations to easily monitor mobile application security performance and focus continuous improvement efforts. BitSight offers solutions for both internal security performance and third-party risk management.

BitSight Mobile AppSec is aligned with recognized industry standards. Magnitudes of vulnerability are reported on the 10-point scale instituted by the Common Vulnerability Scoring System (CVSS). Coverage for the OWASP Mobile Top 10 framework is provided by the security assessments of apps.

Conclusion

Historically, many organizations saw mobile security investment as a necessary, albeit costly, preventative measure. Today, it is increasingly seen as a cost-saving investment or even a revenue driver within the development life-cycle of mobile apps. This has been highlighted in mainstream media, including in Forbes, as well as other industry-specific publications.

Security and privacy are now significant contributors to the brand image of virtually all mobile apps. The recent shake-up in the popular and substantial market for instant-messaging apps illustrates this perfectly—an emerging instant-messaging app focused on security and privacy doubled its user base from 20 million to 40 million in the remarkably brief period between December 2020 and January 2021.

"The integration of security evaluations as a continuous part of the development and release cycle for all mobile apps is an investment app publishers should make in their brand," said Al Rashid.

"Developers can no longer afford to put off security until the last minute or even after the app has been released. Prioritizing mobile application security has become essential to compete in today's market."

Appendix and Heatmaps

HEATMAP **1** | Material and Severe Vulnerability Percentage By Sector (Android)

	Arbitrary Code Execution Probable	Runs Root Command Check	Sensitive Data Certificate Validation	Sensitive Data HTTP Android ID	Sensitive Data HTTP Email	Sensitive Data HTTP GPS Latitude	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IMEI	Sensitive Data HTTP Password	Sensitive Data HTTP Username	Sensitive Data HTTP ZIP Code
Aerospace/Defense	0.0	0.0	0.0	0.0	0.0	0.6	0.6	0.0	0.0	0.0	0.0
Business Services	0.0	0.0	0.1	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0
Consumer Goods	0.2	0.0	0.5	0.0	0.0	0.0	0.0	0.0	0.1	0.1	0.1
Education	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Energy/Resources	0.1	0.0	0.5	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0
Engineering	0.1	0.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0
Finance	0.0	0.0	0.1	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0
Food Production	0.0	0.0	0.5	0.0	0.2	0.2	0.0	0.0	0.2	0.2	0.0
Government/Politics	0.1	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0
Healthcare/Wellness	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Insurance	0.1	0.1	0.2	0.1	0.1	0.1	0.0	0.0	0.0	0.1	0.0
Legal	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Manufacturing	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0
Media/Entertainment	0.2	0.0	0.1	0.0	0.0	0.2	0.1	0.0	0.0	0.0	0.0
Nonprofit/NGO	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Real Estate	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Retail	0.4	0.1	0.5	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0
Technology	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Telecommunications	0.1	0.0	0.5	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0
Tourism/Hospitality	0.0	0.0	0.2	0.1	0.0	0.1	0.0	0.0	0.1	0.1	0.2
Transportation	0.2	0.0	0.3	0.0	0.0	0.1	0.0	0.1	0.0	0.1	0.1
Utilities	0.0	0.2	0.2	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.2

Percentage of Apps Deemed Vulnerable

HEATMAP **2** | Material and Severe Vulnerability Percentage By Sector (iOS)

	Sensitive Data Certificate Validation	Sensitive Data HTTP AdID	Sensitive Data HTTP Email	Sensitive Data HTTP First Name	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IDFV	Sensitive Data HTTP Last Name	Sensitive Data HTTP Password	Sensitive Data HTTP Username	Sensitive Data HTTP ZIP Code	Change Cipher Spec Check
Aerospace/Defense	0.0	0.0	0.0	1.9	3.8	0.0	1.9	0.0	0.0	1.9	0.0
Business Services	0.5	3.0	0.0	0.3	0.1	0.1	0.0	0.1	0.1	0.0	0.0
Consumer Goods	1.0	1.0	0.0	0.2	0.0	0.5	0.0	0.2	0.0	0.0	0.0
Education	0.4	0.3	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Energy/Resources	0.6	0.0	0.0	0.0	0.0	0.6	0.0	0.0	0.0	0.0	0.0
Engineering	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Finance	0.7	0.5	0.0	0.1	0.2	0.3	0.0	0.1	0.1	0.0	0.1
Food Production	0.0	0.5	0.0	0.5	0.5	0.5	0.0	0.5	0.5	0.0	0.0
Government/Politics	0.8	0.2	0.0	0.2	0.0	0.2	0.0	0.0	0.0	0.0	0.0
Healthcare/Wellness	0.3	0.0	0.1	0.0	0.0	0.2	0.0	0.1	0.1	0.0	0.0
Insurance	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Legal	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Manufacturing	0.0	0.0	0.0	0.2	0.2	0.2	0.0	0.0	0.2	0.0	0.0
Media/Entertainment	0.5	2.6	0.0	2.2	0.2	0.9	0.0	0.0	0.0	0.2	0.0
Nonprofit/NGO	0.9	0.0	0.0	0.9	0.9	0.0	0.0	0.0	0.0	0.5	0.0
Real Estate	1.0	1.0	0.0	0.0	0.5	1.0	0.0	0.0	0.0	1.0	0.0
Retail	2.0	1.2	0.0	0.0	0.5	0.8	0.0	0.0	0.0	0.0	0.0
Technology	0.6	1.0	0.0	0.1	0.3	0.7	0.0	0.1	0.1	0.0	0.0
Telecommunications	1.0	1.1	0.1	0.8	0.2	1.0	0.0	0.1	0.1	0.1	0.1
Tourism/Hospitality	1.4	0.5	0.0	1.0	0.1	0.4	0.1	0.0	0.0	0.2	0.0
Transportation	2.3	0.8	0.0	0.2	0.3	1.6	0.0	0.0	0.0	0.2	0.0
Utilities	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Percentage of Apps Deemed Vulnerable

3.2 — 2.4 — 1.6 — 0.8 — 0.0

HEATMAP 3 | Material and Severe Vulnerability Percentage by App Genre (Android)

	Arbitrary Code Execution Probable	Runs Root Command Check	Sensitive Data Certificate Validation	Sensitive Data HTTP Android ID	Sensitive Data HTTP Email	Sensitive Data HTTP GPS Latitude	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IMEI	Sensitive Data HTTP Password	Sensitive Data HTTP Username	Sensitive Data HTTP WiFi IP	Sensitive Data HTTP ZIP Code
Book	0.1	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Business	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Communication	0.1	0.0	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Education	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Entertainment	0.1	0.0	0.2	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.1	0.1
Finance	0.0	0.0	0.2	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Food & Drink	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Health & Fitness	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Lifestyle	0.0	0.1	0.2	0.0	0.0	0.1	0.0	0.0	0.1	0.0	0.0	0.0
Medical	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
News	0.3	0.0	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Productivity	0.1	0.0	0.2	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Reference	0.1	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Shopping	0.1	0.0	0.5	0.0	0.0	0.3	0.0	0.0	0.0	0.0	0.0	0.0
Social	0.0	0.0	0.1	0.0	0.0	0.2	0.2	0.0	0.0	0.0	0.0	0.0
Sports	0.1	0.0	0.0	0.1	0.1	0.2	0.1	0.0	0.1	0.1	0.0	0.1
Tools	0.1	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Travel	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.1

Percentage of Apps Deemed Vulnerable (scale 0.0 – 0.5)

HEATMAP **4** | Material and Severe Vulnerability Percentage by App Genre (iOS)

HEATMAP **5** | Material and Severe Vulnerability Percentage by App Popularity (Android)

HEATMAP **6** | Material and Severe Vulnerability Percentage by App Popularity (iOS)

	Sensitive Data Certificate Validation	Sensitive Data HTTP AdID	Sensitive Data HTTP Email	Sensitive Data HTTP First Name	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IDFV	Sensitive Data HTTP Last Name	Sensitive Data HTTP Password	Sensitive Data HTTP Username	Sensitive Data HTTP ZIP Code	Change Cipher Spec Check
1	0.3	0.4	0.0	0.3	0.5	0.3	0.0	0.1	0.1	0.1	0.0
1 < x <= 10	0.5	0.4	0.0	0.4	0.2	0.3	0.0	0.0	0.0	0.0	0.0
10 < x <= 100	0.8	0.5	0.0	0.7	0.1	0.6	0.0	0.0	0.0	0.1	0.1
100 < x <= 1K	0.9	1.1	0.0	0.5	0.1	0.7	0.0	0.1	0.1	0.1	0.1
1K < x <= 10K	1.2	2.1	0.0	0.5	0.4	0.8	0.1	0.0	0.0	0.1	0.0
10K < x <= 100K	1.6	2.0	0.1	0.5	0.3	1.6	0.0	0.1	0.1	0.4	0.0
100K < x <= 1M	1.2	1.9	0.0	0.6	0.1	1.5	0.0	0.0	0.0	0.0	0.0
1M < x <= 10M	0.6	4.1	0.0	0.0	0.0	2.9	0.0	0.0	0.0	0.0	0.0
10M < x <= 100M	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Color scale: Percentage of Apps Deemed Vulnerable (0.0 – 4.0)

HEATMAP **7** | Material and Severe Vulnerability Remediation By Sector (Android)

	Arbitrary Code Execution Probable	Runs Root Command Check	Sensitive Data Certificate Validation	Sensitive Data HTTP Android ID	Sensitive Data HTTP GPS Latitude	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IMEI
Aerospace/Defense	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Business Services	0.0	0.0	0.1	0.0	0.1	0.0	0.0
Consumer Goods	0.3	0.1	0.0	0.0	0.2	0.0	0.0
Education	0.0	0.0	0.1	0.0	0.0	0.0	0.0
Energy/Resources	0.0	0.0	0.1	0.0	0.0	0.0	0.0
Engineering	0.0	0.0	0.2	0.0	0.1	0.1	0.0
Finance	0.0	0.2	0.2	0.0	0.1	0.0	0.0
Food Production	0.0	0.3	0.3	0.2	0.0	0.0	0.0
Government/Politics	0.0	0.0	0.1	0.0	0.1	0.0	0.0
Healthcare/Wellness	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Insurance	0.1	0.1	0.1	0.1	0.0	0.0	0.1
Legal	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Manufacturing	0.0	0.0	0.1	0.0	0.1	0.0	0.0
Media/Entertainment	0.5	0.0	0.3	0.3	0.1	0.0	0.0
Nonprofit/NGO	0.0	0.0	0.1	0.0	0.2	0.0	0.0
Real Estate	0.0	0.0	0.0	0.2	0.9	0.0	0.0
Retail	0.0	0.2	0.2	0.1	0.4	0.1	0.1
Technology	0.2	0.0	0.2	0.1	0.1	0.0	0.0
Telecommunications	0.0	0.2	0.3	0.2	0.3	0.0	0.0
Tourism/Hospitality	0.1	0.0	0.4	0.1	0.1	0.0	0.0
Transportation	0.0	0.0	0.3	0.1	0.2	0.0	0.0
Utilities	0.0	0.0	0.0	0.2	0.2	0.0	0.0

Percentage of Apps Deemed Remedied — scale: 0.00, 0.15, 0.30, 0.45, 0.60, 0.75, 0.90

HEATMAP **8** | Material and Severe Vulnerability Remediation By Sector (iOS)

Sector	Sensitive Data Certificate Validation	Sensitive Data HTTP AdID	Sensitive Data HTTP Email	Sensitive Data HTTP First Name	Sensitive Data HTTP GPS Longitude	Sensitive Data HTTP IDFV	Sensitive Data HTTP Last Name	Sensitive Data HTTP Password	Sensitive Data HTTP Username	Sensitive Data HTTP ZIP Code
Aerospace/Defense	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Business Services	0.1	0.1	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0
Consumer Goods	0.0	0.2	0.0	0.0	0.5	0.2	0.0	0.0	0.0	0.2
Education	0.0	0.0	0.1	0.1	0.0	0.0	0.1	0.0	0.1	0.0
Energy/Resources	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Engineering	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Finance	0.6	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Food Production	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Government/Politics	0.0	0.0	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.0
Healthcare/Wellness	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1
Insurance	0.0	0.3	0.0	0.0	0.0	0.3	0.0	0.0	0.0	0.0
Legal	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Manufacturing	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Media/Entertainment	0.1	0.7	0.0	0.4	0.2	0.8	0.0	0.0	0.0	0.1
Nonprofit/NGO	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Real Estate	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.0	0.0
Retail	0.3	0.6	0.0	0.2	0.3	0.0	0.0	0.0	0.0	0.6
Technology	0.3	0.3	0.0	0.0	0.1	0.2	0.0	0.0	0.0	0.0
Telecommunications	1.0	0.8	0.0	0.0	0.1	0.1	0.0	0.0	0.0	0.0
Tourism/Hospitality	0.1	0.0	0.1	0.4	0.2	0.1	0.4	0.1	0.1	0.1
Transportation	1.0	0.8	0.0	0.0	0.3	1.0	0.0	0.0	0.0	0.2
Utilities	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Percentage of Apps Deemed Remedied (scale 0.0 – 1.0)

BitSight Insights

BitSight Insights provides objective, trusted data and analytics on global, national, and sectoral cybersecurity performance to improve public awareness of cyber risk and enhance public access to the highest quality security performance data.

Abdullah Al Rashid, Andrew Burton, Maham Haroon, Tom Montroy, Jake Olcott, and Pedro Umbelino (a-z) contributed to this report.

BITSIGHT®
The Standard in **SECURITY RATINGS**

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight is transforming the way that the global marketplace addresses cyber risk with cybersecurity ratings and analytics. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third party risk; underwrite cyber insurance policies; conduct financial diligence; and improve national security. With 2,300 global customers and the largest ecosystem of users and information, BitSight is the Standard in Security Ratings. Learn more at bitsight.com.