Artifact Evaluated
NDSS
Available
Functional
Reproduced

50 Shades of Support: A Device-Centric Analysis of Android Security Updates

Abbas Acar[*], Güliz Seray Tuncay[§], Esteban Luques[*], Harun Oz[*], Ahmet Aris[*], and Selcuk Uluagac[*]
[*]Cyber-Physical Systems Security Lab, Florida International University, Miami, Florida, USA
[§]Google, Mountain View, CA, USA
{aacar001, eluqu004, hoz001, aaris, suluagac}@fiu.edu, gulizseray@google.com

***Abstract*—Android is by far the most popular OS with over three billion active mobile devices. As in any software, uncovering vulnerabilities on Android devices and applying timely patches are both critical. Android Open Source Project has initiated efforts to improve the traceability of security updates through Security Patch Levels assigned to devices. While this initiative provided better traceability for the vulnerabilities, it has not entirely resolved the issues related to the timeliness and availability of security updates for end users. Recent studies on Android security updates have focused on the issue of delay during the security update roll-out, largely attributing this to factors related to fragmentation. However, these studies fail to capture the entire Android ecosystem as they primarily examine flagship devices or do not paint a comprehensive picture of the Android devices' lifecycle due to the datasets spanning over a short timeframe. To address this gap in the literature, we utilize a device-centric approach to analyze the security update behavior of Android devices. Our approach aims to understand the security update distribution behavior of Original Equipment Manufacturers (OEM) by using a representative set of devices from each OEM and characterize the complete lifecycle of an average Android device. We obtained 367K official security update records from public sources, spanning from 2014 to 2023. Our dataset contains 599 unique devices from four major OEMs that are used in 97 countries and are associated with 109 carriers. We identify significant differences in the roll-out of security updates across different OEMs, device models and types, and geographical regions across the world. Our findings show that the reasons for the delay in the roll-out of security updates are not limited to fragmentation but also involve several OEM-specific factors such as the type of support the device receives (e.g., monthly, quarterly, biannual). Our analysis also uncovers certain key issues regarding the security update distribution that can be readily addressed as well as exemplary practices that can be immediately adopted by OEMs in practice.**

I. Introduction

Like any other software, Android can have vulnerabilities with varying severity levels that can negatively impact its users [19], [77], [78]. Patches to these vulnerabilities come from various sources such as Linux, Google, and Original Equipment Manufacturers (OEMs) (e.g., Samsung, Xiaomi, Oppo) [13]. To date, there are more than 4K vulnerabilities published for Android [1]. This constant stream of vulnerabilities requires periodic security updates. Android Open Source Project (AOSP) publishes a monthly Android Security Bulletin (ASB) containing the vulnerabilities and their patches [11] for the ecosystem to track them from a single source. After Google releases the ASB, OEMs patch their device-specific vulnerabilities, then the mobile carriers (e.g., Verizon, T-mobile) apply their customization, if there is any, before the security updates are rolled out to the end users.

User Concerns. Unfortunately, a straightforward security update rollout process becomes cumbersome with every new device/model released by OEMs. Samsung has a billion active users [75] with 1400 unique models (e.g., `SM-970U`) of 402 devices (e.g., `Galaxy S22`) associated with 97 countries and 109 carriers. When we consider all unique model and country-carrier combinations, this requires the creation, customization, and testing of approximately 20K variations of each security update periodically (e.g., monthly). Other OEMs (e.g., Xiaomi), though on a smaller scale, also operate in many regions with large sets of end users. This workload is causing irregularities in the security update support of end-user devices, such as delays in the security update process or the failure to deliver the security updates at all for some models. The end users suffering from these issues express them in the community forums; the issues are sometimes specific to certain regions [2], [3], models [4], or carriers [5]. Hence, one of our goals in this study is to understand the factors that impact the distribution and lack of updates, which is crucial for improving the security of the Android ecosystem.

Knowledge Gap in the Literature. Several studies in the literature focused on the roll-out of Android security updates [87], [35], [34]. These studies either focused on the end-to-end delay for a specific vulnerability type (e.g., kernel vulnerabilities) [87] or the contribution to delay by different stakeholders (e.g., manufacturers, carriers, end-users) [35], [34]. However, they largely ignored 1) the entire lifecycle of the devices and 2) the non-flagship devices, depicting an *incomplete picture* of the Android ecosystem. For example, [35] reports a delay of 24 days by manufacturer and carrier. However, this finding, as we found in our study, is only correct for monthly-supported devices while it increases to 41 and 63 days for devices with different support types like quarterly or biannual support. We found that the release delay can go up to 300 days for some of the currently supported devices (Section IV). Moreover, the earlier studies mostly attributed the reason for the delay to fragmentation, but largely ignored factors like support type, device model, and region on the availability and timeliness of the security updates.

Network and Distributed System Security (NDSS) Symposium 2024
26 February - 1 March 2024, San Diego, CA, USA
ISBN 1-891562-93-2
https://dx.doi.org/10.14722/ndss.2024.24175
www.ndss-symposium.org

In this work, we conduct a device-centric analysis of Android security updates. The goal of this device-centric approach is to understand the entire lifecycle of Android devices, including periods beyond monthly support, and to characterize the practices of Android OEMs using a large, representative set of devices, extending beyond just the flagship models. Moreover, our analysis seeks to uncover the various factors impacting the Android security support lifecycle across different OEMs. Our dataset, assembled from publicly available official sources, includes 367K security updates for a broad range of 599 devices released between 2014 (prior to the first Android Security Bulletin) and 2023. Our objectives in this study are to answer the following research questions:

RQ1: How does the maintenance chronicle of Android devices look like throughout their lifecycle? (§IV)

RQ2: What factors impact the distribution of security updates of Android devices during their support period? (§IV-A,§V)

RQ3: What potential risks do unpatched Android devices pose, and when do they become unsafe to use? (§IV-B)

RQ4: What are the immediate issues causing user concerns in practice, and what exemplary practices can be broadly adopted by all OEMs? (§VI)

To answer these research questions, we performed our analysis with the security updates from the top three OEMs (i.e., Samsung, Xiaomi, and Oppo) as well as Google, which is the primary developer of Android and an OEM that has not exposed itself to fragmentation issues. We found that Android devices do not have a single support type in practice, but rather, depending on the OEM, they go through monthly, quarterly, and biannual security support periods, throughout their lifetime, then reach their End-of-Life (EOL). The support type mainly impacts the update frequency, but we found in this paper that it also impacts the number of security updates, support duration, and the release delay of the security updates. Even within the same support type, a security update may reach the end user with a delay or may not reach them at all due to several factors such as 1) geolocation, 2) carrier association, 3) device type, or 4) whether the device is supported by partnership agreements. We also found significant differences in the device support policies and the distribution of security updates among OEMs. For example, Samsung, as the largest OEM offering a broad spectrum of devices, exhibits significant variance in security update behaviors depending on factors such as the support type, device's intended geolocation, and device type. On the other hand, Oppo and Xiaomi offer relatively fewer security updates for a shorter support duration. In contrast, Google, with its limited number of devices in the market, provides regular monthly security updates throughout the lifetime of an Android device, independent of these impacting factors.

While being so crucial for the safety of the user, many Android devices receive security updates only for a few years. As of 2020, more than one billion Android devices were estimated not to receive security patches anymore [52]. Since such devices are still functional, users continue using their Android devices, which leaves them at risk of being open to known vulnerabilities [33]. Half of the zero-day vulnerabilities seen in the wild by Google during 2022 were variants of previously patched vulnerabilities [16]. Not only unsupported devices but also supported devices that missed security updates for a certain duration will be open to these vulnerabilities. Hence, we study the risks associated with using unpatched Android devices. Our findings show that vulnerabilities impacting the devices tend to arise immediately after the end of the support, reaching up to 50 critical CVEs in two years. We found that a large percentage (89%) of these vulnerabilities can be exploited without user interaction and some (27%) can even be exploited remotely without the attacker having to invest much effort, leaving the users, their devices, and even app developers [81] open to attackers.

Our findings also revealed other key issues regarding the Android security update process, especially those causing user concerns in practice. We found that OEMs appear to lack uniformity in implementing best practices, and even within a single OEM's processes, inconsistencies are often noticeable. We found variations in the support behavior observed by different models and pairs, discrepancies in support lists, discrepancies in the partnership agreements, and misleading announcements as key issues that can be immediately fixed by OEMs. Moreover, we found that despite the recommendation by the Federal Trade Commission [22], only Google provides a guaranteed support date for all devices. Recently, with Android Enterprise Recommended (AER) [9] devices, this practice is implemented by more OEMs, but it is done so only for a limited number of devices. On the other hand, some OEMs like Xiaomi and Google also publish End-of-Support (EOS) product lists, in which the users can make better-informed decisions when deciding on which devices to use.

The main contributions of this work are as follows:

- We utilize the largest official dataset in the literature (∼367K security updates covering 599 devices, 97 countries, and 109 carriers) to characterize the Android security updates. The size and duration of this dataset allow us to provide a complete picture of the Android ecosystem and explore the full lifecycle of devices.
- Our analysis revealed several crucial factors that affect the availability and timeliness of Android security updates such as support type, geolocation, device type, and partnership agreements across different OEMs.
- For the first time in the literature, we investigated the security posture of unpatched Android devices.
- We also pinpointed key issues and inconsistencies in the security update process that have been causing practical difficulties for users and highlighted exemplary practices implemented by some of the OEMs in our dataset.
- Finally, we released both the dataset and the code necessary to fully reproduce the results presented in this paper.[1]

II. Security Updates in Android Ecosystem

In this section, we cover the necessary background information about the security updates in the Android ecosystem.

A. Security Update Rollout Process

The vulnerabilities in the Android ecosystem can be discovered by anybody. The most common reporters of the vulnerabilities are Google (internally), AOSP partners (e.g.,

[1] https://github.com/cslfiu/Android-Security-Updates

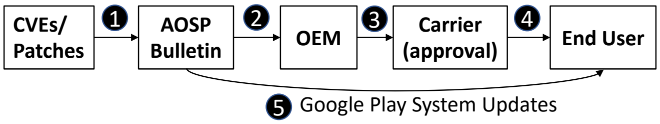


Fig. 1: Security Update Rollout Process in Android.

OEMs, chip makers, carriers), and independent researchers. These vulnerabilities are being reported to AOSP [24] as well as to vulnerability databases, in which each vulnerability is assigned a unique CVE identifier. Figure 1 shows the security update rollout process in Android. AOSP publishes the monthly Android Security Bulletin (ASB) containing both the vulnerabilities and their patches (❶). The vulnerabilities include Android system vulnerabilities as well as other vulnerabilities such as the kernel, chipset, or OEM-specific vulnerabilities [13]. Once the monthly ASB is published by AOSP, an OEM applies all the patches that impact its devices (❷). During this step, the OEM sets the Security Patch Level (SPL) parameter through the system property *ro.build.version.security_patch* on the security update that will be delivered to the end user. The OEM also applies their customization on top of the Google released patch and performs the compatibility tests [25] (❸). Afterwards, though it may vary between the carriers, the carrier approves the final update that will be sent to the end user for carrier-branded devices (❹). However, OEM-branded devices receive updates directly from the OEM without carrier approval. Moreover, it is also important to note that Pixel devices do not go through any OEM optimization, therefore, eliminating the delay in this step. Once the firmware[2] containing the patches is made available by the OEM/carrier, the end user installs it via an over-the-air (OTA) update [27]. The exception is the security updates through the Project Mainline which can be pushed directly to the end user via the Google Play system services (❺). However, the updates through the Google Play system services can be applied only to the vulnerabilities in the supported modules [12].

B. Types of Security Updates

Each ASB includes a Security Patch Level (SPL), which is standardized data in string format to track the security level across the OEMs, devices, and end users. This date closely corresponds to the date the ASB–which includes the most recent patches–is published, although it can be a few days off from the actual publication date. There are four methods through which patches to Android vulnerabilities can be delivered to the end user: partial SPL, complete SPL, major OS upgrade, and Google Play system updates.

Partial and Complete SPL. ASBs include two SPLs: partial and complete SPL [13]. Partial SPL ends with “-01” (e.g., `YYYY-MM-01`) and contains only the vulnerabilities in Android system components while the complete SPL ends with “-05” (e.g., `YYYY-MM-05`) and addresses not only the vulnerabilities in Android system components but also those that are product-specific or originate from the closed-source components such as the Qualcomm chips. The security level promised by the complete SPL is stronger as it addresses a greater number of vulnerabilities.

Major OS Upgrades. Similar to SPLs, major OS upgrades can contain security enhancements and vulnerability patches. They are generally published once a year and contain patches for 100-200 CVEs. So far, the ASB included CVEs patched through Android 10, Android 11, Android 12, Android 12L, and Android 13. Similar to partial SPLs, major OS upgrades only include the generic OS updates so they can be directly rolled out to the OEMs and carriers, and then finally to the end users.

Google Play System Updates (Project Mainline). Project Mainline is introduced with Android 10 [10]. It modularizes some of the Android system components and enables AOSP to push security updates directly to the end user through the Google Play system services. Currently, 25 components are modularized. The patches to CVEs deployed through the Google Play System Updates are published in the ASB under the partial SPL [11] together with the impacted component.

Partial SPLs mostly affect the Android system components; hence, OEMs do not need to apply any additional patches or customization before they roll these out to the end users. Similarly, major OS upgrades can be rolled out to the end users with minimal customization from the OEM. However, although the complete SPL provides a stronger security level, it takes device manufacturers longer to apply it since all the device-specific patches need to be applied. Therefore, some OEMs may prefer to use the partial SPL instead of the complete SPL for the faster delivery of available patches. We found that Samsung, Xiaomi, and Oppo use the partial SPL on the firmware while Google uses the complete SPL on its updates [26].

C. Announcement and Delivery of Security Updates

In order to deliver the security updates securely to the end users, OEMs use various practices, such as integrity checks through cryptographic signatures, customized compression, or encryption techniques. For instance, we found that all OEMs name the firmware by partially including the hash for the integrity check. We found Oppo employs a .ozip format to protect the firmware and uses model-specific encryption keys to hinder unauthorized modifications [48]. Xiaomi provides an API for the latest updates, which includes a download link for the firmware [84]. Oppo also includes a download link for the latest update on its website [48]. Google, on the other hand, publishes all firmware updates on a dedicated webpage [30].

OEMs handle security update announcements in different ways. For instance, Oppo and Xiaomi do not typically include the SPL in their historical announcements [48]. In contrast, Samsung includes the SPL in all their security update announcements and Google includes a tag and build number in its updates, which can be matched with the corresponding SPL value via another table [29]. For this reason, while we were able to obtain the SPL from the announcement for Samsung and Google, we needed to download the actual firmware for Oppo and Xiaomi to extract the SPL during dataset procurement.

[2] By ”firmware” or ”security update” or ”OTA update,” we refer to the System Firmware Images or OTA images that include the Android OS, system apps, OEM customizations, and updates to the device-specific firmware.

TABLE I: Official Security Updates Dataset Statistics.

OEM	Security Updates				
	Total	**Unique Device**	**Region/Country**	**Carrier**	**Duration**
Samsung	354165	275	97 countries	109	Apr 2015 - Mar 2023
Xiaomi	2286	223	10 regions*	-	Dec 2014 - Jun 2023
Oppo	9241	72	35 countries	-	Jan 2018 - Aug 2022
Google	900	20	12 regions**	27**	Nov 2015 - Mar 2023
Total	**366592**	**599**			

*Xiaomi regions include individual countries and region definitions like Global and EEA.
**This is the lower bound since we only counted the explicitly given countries/carriers.

OEMs also announce the list of the devices they support in a separate website. Xiaomi announces End of Service (EOS), Android Enterprise Recommended (AER) devices, and the patched CVEs among other details. Oppo follows a similar practice in its announcements. It is also worth mentioning that different OEMs use different SPL types in their firmware. We found that Xiaomi, Oppo, and Samsung typically use partial SPLs in their firmware, while Google utilizes the complete SPL in their firmware.

III. Dataset

We utilize the datasets released by OEMs to satisfy three requirements. First, the data should be *official* for reliable results. Second, the device data should include the *complete* history because missing updates would give misleading results. Third, the data should be large enough to be *representative* for the given OEM or carrier. With these requirements in mind, we collected the datasets from Google, Samsung, Oppo, and Xiaomi for this study.

A. History of Security Updates

We downloaded the security updates for each OEM using the following methodologies:

Samsung: Samsung announces both security updates including regular maintenance updates and major OS upgrades in a dedicated webpage for each pair (e.g., `SM-F926U1/TMB` [66]). Each `<model/CSC>` pair has a unique URL containing all its security updates. Here, CSC is a Samsung code that mainly describes the country or the combined country-carrier pair for which the device is intended. To fetch all the announcements, we constructed all possible URLs using the official models [57] and community-compiled list of CSC values [8]. We queried the database for almost half a million pairs. We identified 21461 pairs (e.g., `SM-F926U1/TMB`) and downloaded their security update history. These pairs contained a total of 354K unique security updates, spanning from April 2015 to March 2023. 343K of them included an SPL value while 11K did not have an SPL value in the security update. In addition to the SPL value, each announcement also includes the *release date* of the firmware build. We used the release dates as the date on which the firmware containing the security update was made available. In addition, each announcement also includes the *Android version* corresponding to the Android version that the patch was applied on. If the security update comes with a new OS, we classify it as a major OS upgrade.

Xiaomi: Xiaomi releases the latest available firmware via an official API [84]. We downloaded the historical data from a third-party website [85] that has been fetching the official security updates every six hours since 2018. We verified the latest update with the currently available firmware list and devices from the official API. In total, this dataset includes 2286 official security updates, spanning from December 2014 to June 2023. We found that Xiaomi releases firmware for 10 regions. China, Global, Russia, and the European Economic Area (EEA) are the most common regions in Xiaomi's security updates history dataset. Unlike Samsung, Xiaomi devices have regional names [86]. For instance, `Redmi K20` is used in China and India, while it is referred to as `Mi 9T` in Hong Kong and Taiwan. We used Xiaomi's given codenames to uniquely identify the devices rather than their public names. In our list, we had a total of 223 unique devices. Since not all the models are available in all regions, we concluded with a total of 756 model-region pairs.

Oppo: Oppo releases the firmware updates for each device in their regional software update website (e.g., updates for Oppo A11k used in India [45]). We constructed all country-device pairs and queried for available pairs. We collected data from 1124 country-device pairs containing 9241 security updates for 72 devices used across 35 countries. Each firmware includes an update date, which we used as a release date. However, Oppo only releases the change log including the SPL for the latest release. Therefore, we downloaded all the firmware to extract the SPL from the configuration files. Oppo does not specify the carrier for which the firmware is intended.

Google: Google releases the firmware images for Pixel and Nexus devices in a dedicated website [30]. Firmware images are released as factory images and full OTA images. We only used full OTA images as we aim to characterize the updates received by the regular end user. We also excluded Nexus devices since shortly after the ASB started, Nexus devices were discontinued by Google. We ended up with 900 full OTA images belonging to 20 devices. Each firmware includes the build date, which we use as the release date of the security updates. We extracted the SPL value of each firmware by using another table released by Google [29], which provides the SPL for each build number. Although Google does not specify the region, they sometimes specify the carrier for which the firmware is intended. Despite its limited market share, we examine Google in this paper because as the primary developer of Android, Google is not subject to the fragmentation issues common to other OEMs and typically sets the standard for security update practices. Therefore, our analysis of Google aims to establish a baseline rather than to offer a comparative evaluation with other OEMs.

B. Support Lists

OEMs inform the users about supported devices through the support lists. Samsung publishes the devices that will receive monthly, quarterly, and biannual support as well as the wearable devices that receive security updates [70]. We downloaded 508 snapshots of this list from Wayback Machine [38], whose dates range from October 2017 to April 2023 with a total of 258 unique devices included. This corresponds to an average of four days between each snapshot which would give us enough granularity for the list updates. Oppo

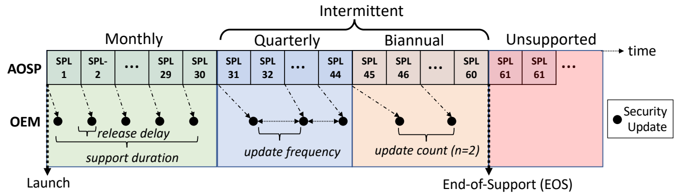


Fig. 2: A representative illustration of the support lifecycle of an Android device.

follows a similar approach and publishes monthly and quarterly supported device lists [49]. We downloaded 17 snapshots of Oppo support lists from January 2021 to March 2023. A total of 208 unique Oppo devices are included in these lists. On the other hand, we were able to retrieve eight snapshots of Xiaomi's monthly and quarterly supported device lists for only two years (2021-2022). In these lists, Xiaomi included 52 unique devices. After 2022, Xiaomi changed its support policy style and began publishing the EOL product list [83]. Finally, Google publishes the guaranteed security update date for Nexus [28] and Pixel [32] devices. The lists include all the devices released by Google so far. We use the support lists to better understand the expected support behavior of the devices and characterize the support types.

IV. Maintenance Chronicle of Android Devices

Samsung [70], Xiaomi [83], and Oppo [49] categorizes their supported devices based on the support frequency, which we call *support type* throughout this paper. Xiaomi and Oppo use monthly and quarterly frequencies, while Samsung also includes a biannual frequency as a support type. We note that most Samsung devices, often associated with price-tier as well, initially receive monthly security updates and then gradually shift to a less frequent schedule, such as quarterly or biannual updates, over a few years. Google, in contrast, provides three years of monthly support for its devices independent of the region, carrier, and device status (i.e., flagship or not) [32]. Finally, Android devices stop receiving security updates after a few years regardless of being operational. A representative diagram illustrating the lifecycle of Android devices is provided in Figure 2.

We use four different metrics to evaluate the efficiency of the security updates received by a device. *Update count* is the number of security updates received during the given support period. *Support duration* is the actual duration between the first and the last security update. We also calculate the support duration per support type. In this case, support duration for a given support type corresponds to the duration between the first and last security update within that support type. Figure 2 illustrates the monthly support duration. In addition, we also calculated the *update frequency*, which shows the average duration between the security updates and *release delay*, which is the duration between the release of SPL by AOSP and the release of the firmware containing that SPL by the OEM. We consider these metrics when assessing the effectiveness of support, as timely and regular delivery of each SPL is just as important as delivering the SPL.

We note that the behavior observed by the end users may differ from the OEM's schedule as the end user starts receiving the security updates from the point of sale, not since the release date. However, our focus in this study is on OEM behavior, and analyzing end-user behavior is out of the scope of this study.

A. Part-1: Supported Period

1) Samsung: Here, we used the entire Samsung security update history (354K) and calculated the update count, support duration, update frequency, and release delay for all pairs (21461). On average, a Samsung device receives 16.5 security updates throughout its lifetime, and 2.5 of them are major OS upgrades. Overall, most devices receive less than 38 security updates throughout their lifetime, with only six devices averaging more than 38. Those are `Galaxy Fold 5G`, `Galaxy S10`, `Galaxy S10+`, `Galaxy S10e`, `Galaxy S20 5G`, `Galaxy S20+ 5G`, and `Galaxy S20 Ultra`. We found that `Galaxy Fold 5G`, `Galaxy S10`, `Galaxy S10+`, and `Galaxy S10e` were released together with Android 9 while `Galaxy S20 5G`, `Galaxy S20+ 5G`, and `Galaxy S20 Ultra` were released with Android 10. Most pairs of these devices received four major OS upgrades as well. Since Android 8 is the start of the efforts to separate OEM customization from the core OS to perform updates more quickly and efficiently, this shows the impact of this initiative.

The average support duration for all Samsung devices is 757 days. Out of 275 devices, there are only 10 devices that received a security update for a duration of more than four years while three devices (i.e., `Galaxy S8`, `Galaxy S8+`, and `Galaxy Tab A Plus 9.7`) received more than five years. Out of all pairs, 18 pairs received more than six years of security support. Interestingly, among those 18 pairs that received more than six years of support, 13 of them have CSC belonging to South Korea, four of them belonging to Taiwan, and one belonging to Hong Kong. This indicates a trend towards a longer support duration for devices used in Eastern Asian countries. It is worth mentioning that these numbers can be considered as a lower bound[3] rather than the actual support duration as they likely receive more security updates.

The average update frequency of all Samsung devices is 50 days, i.e., devices receive a security update every 50 days. The average update frequency of most devices is shorter than 200 days, while it is longer than 200 days for only five devices, which are `Galaxy On7 (2015)`, `Galaxy Tab A Plus 9.7`, `Galaxy S6`, `Galaxy S6 edge`, `Galaxy Tab E 8.0`. The frequency is the main metric affected by the support type (e.g., monthly). We will further analyze the impact of the support type in Section V-A.

Regarding the release delay, we are interested in the delay between the Security Patch Level (SPL) and the release of the firmware by the OEM; therefore, we excluded the announcements without an SPL value. We calculated the release delay for 20943 pairs out of 21461 pairs. The average release delay of all Samsung devices is 140 days, meaning that the firmware for the devices is ready to be rolled out to the end user 140 days after the release of SPL. Out of 256 devices, 211 devices have an average release delay of fewer than 70 days. The remaining

[3] We call it ”lower bound” because post-publication updates can increase these numbers.

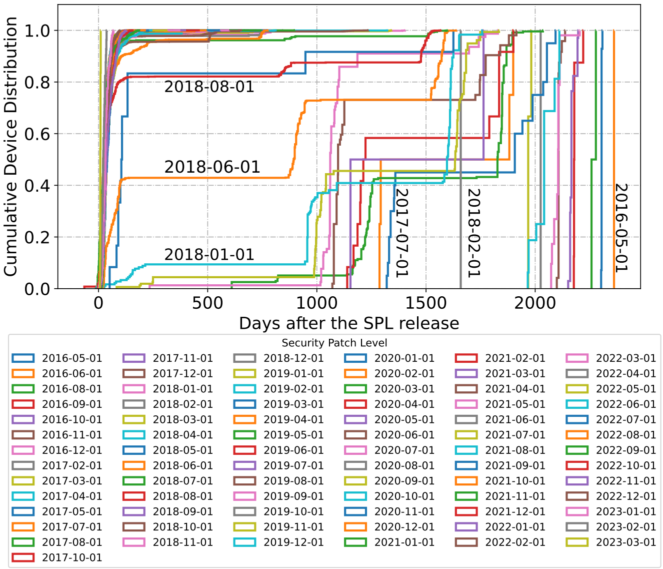


Fig. 3: Cumulative distribution of SPLs on Samsung devices over time. The figure illustrates three distinct SPL assignment behaviors: initial batch assignments after 2000 days for SPLs between 2016-05 and 2017-05, two-phase batches for SPLs between 2017-05 and 2018-05, and a more consistent rollout for SPLs post 2018-06, with a majority of devices updated within 70 days.

45 devices have an average delay ranging from 72 days to 2112 days.

To further investigate these very long delays, we plot the cumulative device distribution for all SPLs over time in Figure 3. We found that Samsung started to assign SPLs starting from the SPL "2016-05-01" although AOSP started with "2015-08-01". We indentified three distinct behaviors for the SPLs. First, SPLs between "2016-05-01" and "2017-05-01" are assigned as a batch to all devices available after 2000 days of the release of the SPLs. Second, SPLs between "2017-05-01" and "2018-05-01" are assigned to the devices in two batches, one is after 1000-1250 days, then the second one is after 1500-1750 days. Finally, SPLs published after "2018-06-01" to date have a more stable rollout process. Finally, SPLs published after "2018-06-01" reached the majority of devices ($> 50\%$) in around 70 days.

2) Xiaomi: Next, we calculated the features (i.e., metrics) for all Xiaomi pairs (756) of all devices (223 unique devices). Xiaomi devices receive three security updates on average. Out of 756 model-region pairs, 37 pairs received six or more security updates. Interestingly, 35 of them belong to the devices used in China and one of them belongs to Singapore. This shows that there is a tendency for the Xiaomi devices used in China to receive more security updates compared to the other regions offering Xiaomi devices. The average support duration of all Xiaomi devices is 170 days, whereas this average is 274 days for the devices used in China. On average, Xiaomi devices receive a security update every 48 days. However, it is important to consider that this frequency only represents the average for the supported duration. This indeed shows why we need to consider all four metrics when evaluating the support behavior of a device.

On average, Xiaomi releases their updated firmware with 32 days of delay after the release of the SPL by the Android Security Bulletin (i.e., release delay). Similar to Samsung security updates after the SPL "2018-05-01", Xiaomi releases security updates of the same SPL as a batch within a small time frame, i.e., once an SPL is available, the OEM prepares the patches for all regions within a short amount of time, resulting in a similar delay for all regions. Particularly, the averages for all the regions are within the range of 25-33 days. When we investigate Xiaomi's release delay over the years, we observe that the release delay corresponding to the SPL in December 2018 was 163 days, whereas this delay dropped to 40-45 days in the 2020-2021 period, and finally reached 38 and 25 days for 2022 and 2023, respectively. Overall, this shows an improvement in the release delay incurred by Xiaomi over the years similar to Samsung, as shown in Figure 3.

3) Oppo: In this part, we calculated the metrics for all Oppo pairs (1124) of all devices (72). On average, Oppo devices received eight security updates throughout their entire lifetime. `R17 Pro` and `R17` are the only devices that received an average of 20 or more security updates. Five different models of `Reno4`, `Reno3 A`, `Neo 7`, `A57`, and `A54` received only an average of two security updates throughout their lifetime. We found that different models of `Reno4` is not receiving at least for more than a year [48] despite, at the time of writing, being in the quarterly-supported device list [49]. The average support duration of all Oppo devices is 583 days. There are only two devices (i.e., `F7` and `F7 128G`) with more than three years of support duration. Similar to the update count metric, some models of `Reno4` and `A54` have the lowest support duration, despite both devices being in the quarterly-supported device list published by Oppo [49] as of writing this paper.

The average update frequency for all Oppo devices is 85 days; however, `F1 Plus` and `F1` have a frequency higher than 200 days per security update. On the other hand, there are five devices with an update frequency lower than 30 days, which is the frequency of the AOSP bulletin. Three of these devices are a series of `Reno4`, others are `A54` and `F17 Pro`. Although `Reno4` gets frequent updates, as we have seen in the update count and support duration analysis, `Reno4` models are only getting two security updates for a very short time. This shows that it is important to consider all metrics while evaluating the security behavior of the devices. The average release delay for all devices is 35 days. Most devices have a delay of 30-45 days after the release of the SPL by AOSP. Among these devices, `F9` and `F9 Pro` have higher delays than others, with an average delay of 52 days and 54 days, respectively. `Reno4 Lite` used in Indenoseia [46] and `Reno4 F` used in Kazakyshtan [47] both have an exceptionally low delay, which is within 10 days of SPL release. However, both of these devices only received two security updates, limiting any generalization solely based on the release delay.

4) Google: Compared to the top three OEMs we examined so far, Google is the one with the most stable support behavior. All of the Pixel devices receive monthly security updates without any delay or missed SPLs. The security updates of 20 Pixel devices are given in Figure 4. The security updates

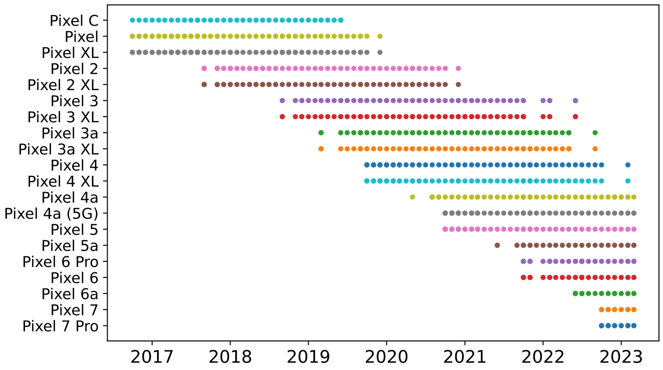


Fig. 4: Security updates for Google Pixel devices.

reported here also align with the support lists given in [32]. However, it is essential to note that Google offers a relatively smaller number of devices compared to the other OEMs. Based on the support lists, only 10 Pixel devices from Google are currently supported [32] as of writing this paper. In contrast, the latest support list indicates that Samsung supports 158 devices, while Xiaomi and Oppo support 52 and 147 devices, respectively.

Takeaway-1: *Overall, our analysis shows that Google maintains a consistent approach by regularly providing monthly security updates throughout the lifetime of an Android device. In contrast, Samsung's security update frequency varies, depending on factors such as the support type, device's age, and others, which we will examine in detail in Section V. Furthermore, Oppo and Xiaomi offer relatively fewer security updates and support their devices for a relatively shorter duration.*

B. Part-2: Unsupported Period

In this section, our goal is to understand the average number of vulnerabilities that may arise in unpatched Android devices, how this number grows over time, and the severity distribution of these vulnerabilities in the unsupported period, during which devices no longer receive security updates.

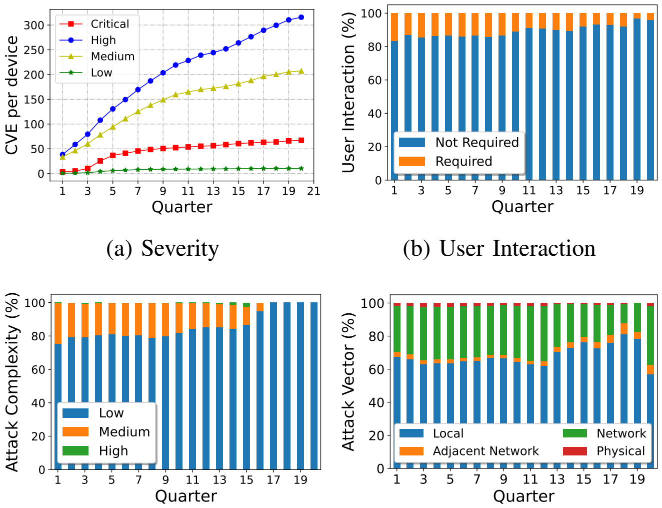
Locating Impacting CVEs. To locate the specific vulnerabilities impacting the devices, we used the last upgraded Android version and the device's chipset. In other words, the device will be vulnerable to any vulnerability affecting its last Android version and any vulnerability impacting its chipset. We obtained the last Android version from the last received security update in the security update history dataset. The chipset information is primarily collected from the OEM's website and supplemented with other public resources. For the vulnerability database, we combined the AOSP bulletin, the Samsung bulletin, and the NIST database. We obtained a list of 2930 CVEs for which we know the impacted Android version and a list of 1649 CVEs which we know the impacted chipset. In total, we were able to assign 4579 CVEs by matching the Android version and the chipset. By the end of this process, we obtained a list of potential CVEs affecting each of the devices in our dataset. Since the ones that are discovered before the EOL will be patched through the security updates, we filter them out using the EOL. However, since manufacturers do not officially announce the EOL date for each device, we calculated the EOL dates using the date of the last security update received by that device. With this approach, we were also able to analyze the devices that have not received security updates for a long time even though they are still on the support list.

Time-based Risk Analysis. To understand the risks associated with continuing to use unpatched Android devices, we separated CVEs received after the last security update into periods of three months (i.e., quarters). On each device, we assigned the CVEs to their corresponding quarter based on the distance between the CVE's publication date and the device's EOL. In other words, we are not concerned with the exact date of the CVE, but with how old the vulnerability is with respect to the device's EOL date. This process yielded a total of thirteen unsupported quarters, which we used to analyze the evolution of vulnerabilities over time. We then used the weighted average counts and added each period's value to those of the previous periods using the cumulative weighted average (CWA): $CWA = \sum_{j=1}^{n} \frac{\sum_{i=1}^{k} m_{ij}}{k_j}$, where m_{ij} is the metric such as CVE count for the i^{th}-device during j^{th}-period. Additionally, n is the maximum number of 3-month periods, and k_j is the number of active devices (with unpatched vulnerabilities) during j^{th}-period.

Risks of Using Unpatched Android Devices. Since we were able to extract the last support dates for each pair, we performed the CVE assignment at the pair level. In total, we had 21461 model-country/carrier pairs from Samsung, 756 model-region pairs from Xiaomi, 1124 country-device pairs from Oppo, and 20 devices from Google. Out of these 23361 pairs from four OEMs, 8594 (36.7%) pairs received at least one CVE impacting the device, which did not receive any security updates for the last three months. The distribution of accumulated CVEs per device during the 20 unsupported quarters ($\sim$ 5 years) is illustrated in Figure 5.

Figure 5a shows the average CVE counts over time by severity for all pairs. On average, an unpatched device will have 76 CVEs in the first quarter reaching 382 CVEs around eight quarters (two years) and 600 CVEs in 20 quarters (five years) without any support. CVEs typically increase immediately after the end of the support. Critical CVEs, which round up to 50, tend to taper off in around two years while medium and high CVEs continue to accumulate throughout the years of unsupported duration while slowing down around three years. Interestingly, the low-severity CVEs remain the lowest throughout the entire unsupported duration.

The distributions of accumulated CVEs on unpatched Android devices grouped by user interaction, attack complexity, and attack vector are given in Figure 5b, 5c, and 5d. Overall, we observed that the no-user-interaction distribution tends to stay above 83% over time with an average of 89%. That is, on average, 89% of the vulnerabilities present in an unpatched device at any given time can be exploited regardless of any user interaction. On the other hand, our analysis revealed that the number of CVEs with high complexity is less than 1%. This indicates that almost all of the vulnerabilities can be exploited with medium or low attack complexity. 67% of the vulnerabilities can be exploited locally, and around 27% can be remotely exploited through the network. On



(a) Severity

(b) User Interaction

(c) Attack Complexity

(d) Attack Vector

Fig. 5: The distribution of accumulated CVEs per device for 20 unsupported quarters (∼ 5 years). On average, an unpatched device is expected to have up to 382 CVEs within two years after the EOL, with 50 of them being critical. 89% of the CVEs do not require user interaction, 86% can be exploited with minimal effort on the attacker's part, while 27% can be exploited remotely.

the other hand, the number of CVEs that require physical connection or connection from the adjacent network is very limited throughout the entire unsupported period.

Case Study. Here, we present a case study to better understand the results of the unpatched device analysis. We analyze `Galaxy Z Fold3 5G` for our study, which is in the list of monthly supported devices as of writing this paper [39]. While most pairs receive security updates, four pairs (i.e., `SM-F926U1/TMB` [66], `SM-F926U1/TMK` [67], `SM-F926U1/XAA` [68], `SM-F926U1/XAG` [69]) belonging to different carriers in the US have not received any security updates for almost the last 10 months. The last security update shows that the devices are with Android 12 and use a Qualcomm SM8350 Snapdragon chipset. We were able to assign 11 CVEs using the chipset and 426 CVEs using the Android version. Then, using the last update date (i.e., EOL), we filtered out the CVEs published before the EOL. We ended up with the 142 CVEs impacting `Galaxy Z Fold3 5`. Among the 142 CVEs, there are six critical and 82 high-severity CVEs. All of these six critical CVEs can be remotely exploited and do not require user interaction. One example is CVE-2023-20946, which impacts the system components of Android due to a remote privilege escalation issue in the Bluetooth settings. Although patches to these CVEs were implemented in AOSP, the end users have never received them. These unpatched vulnerabilities pose a significant risk to users. Similar concerns are also expressed by Google [16], which notes that 50% of the observed zero-days in the first half of 2022 were variants of previously patched vulnerabilities and the attackers are likely to use known vulnerabilities before looking for novel ones.

Takeaway-2: *Overall, our results demonstrate that during the unsupported period, (unpatched) devices continue to receive critical CVEs that can be remotely exploited without requiring any user interaction or too much investment from the attacker. These CVEs tend to arise immediately after the end of support and taper off after two years.*

V. Impacting Factors Analysis

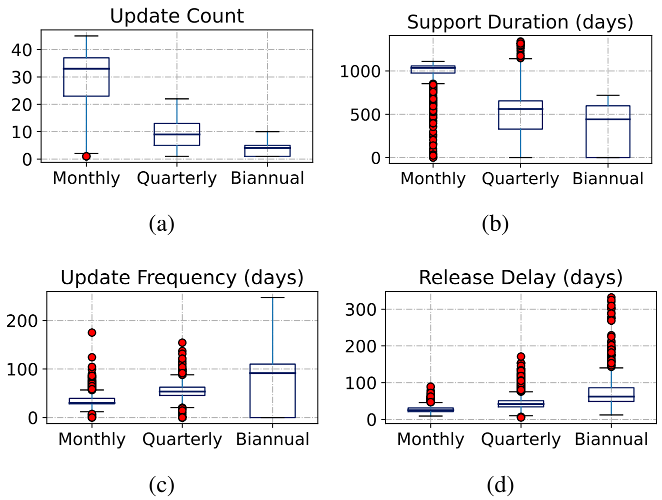
In this section, we examine the impact of the factors such as support type (e.g., monthly, quarterly), geolocation, device type, carrier association, and partnership agreements on the timely delivery of security updates.

A. Support Type

Samsung. Our analysis of the support lists revealed a lifecycle pattern for devices, as illustrated in Figure 2; devices transition from monthly to quarterly and then to biannual support over time. We calculate the support periods by marking the dates devices transition between lists. However, devices from the most recent snapshot in March 2023 are still receiving updates, and those from the first support lists in October 2017 likely began their support earlier. To address this, we identified *completed periods* where both the start and end dates are known, excluding data from the first and last snapshots. This method allowed us to identify 20 devices that completed monthly support, 110 which completed quarterly support, and 50 which completed biannual support. No device completed all three types of support. For instance, `Galaxy S9` had monthly and quarterly support, but its biannual support is still ongoing. `Galaxy Tab A 8 (2019)` completed biannual support but never featured on the monthly support list. Four wearable devices are currently in the support list but have not yet completed the entire support duration.

We first calculated the average support duration for the completed monthly, quarterly, and biannual support periods. We found that the average monthly, quarterly, and biannual support duration are 1044 days, 573 days, and 580 days, respectively. In total, this corresponds to 2197 days (∼ 6 years) of support. While this indicates that the devices stay in the support lists for a duration of six years, it does not necessarily mean that a device will receive security updates for six years in practice. As discussed in Section IV-A, the average support duration is 757 days with only 18 pairs out of 21461 pairs–specifically those used in Eastern Asian countries–having received six years of support.

As previously noted, we were able to extract the monthly support dates for 20 devices, the quarterly support dates for 110 devices, and the biannual support dates for 50 devices. As these periods pertain to individual devices (i.e., `Galaxy S22`), not the models (e.g., `SM-S901E`) or pairs (e.g., `SM-S901E/ZTA`), we used Samsung's official device-model pair list [57] to obtain the specific support dates for each model. Then, we computed the number of security updates received (i.e., update count), the support duration, the update frequency, and the release delay for each support type and pair. In total, the dataset used for the calculation includes 2509, 7470, and 2304 unique pairs for monthly, quarterly, and biannual support periods.



(a)

(b)

(c)

(d)

Fig. 6: Impact of Samsung's support type on security updates.

Figure 6 shows the results for different support types. Overall, there is a direct correlation between the support type and all the metrics we computed. Particularly, the average number of security updates received during monthly support is 33, while it is nine and four for quarterly and biannual support types, respectively. Next, we want to compare the duration that devices stay in the support lists with the actual security updates received. As previously noted in this section, the devices stay in the monthly, quarterly, and biannually support lists for 1044, 573, and 580 days, respectively. However, we found that the median for the support duration in our dataset is 1034, 560, and 442 days for the same support types. This means that although devices receive security updates for almost the entire monthly and quarterly support duration announced by Samsung, their biannual support duration in practice is significantly less than that specified in the support list.

For the security update frequency, the expected value is 30, 90, and 180 days for the monthly, quarterly, and biannual support types, respectively as their names imply. However, we found that the median frequency is 30 days, 53 days, and 91 days, for monthly, quarterly, and biannually supported devices, respectively. Therefore, in this context, we can conclude that the update frequency of different support types is better in practice than what their names imply. Finally, the support type also impacts the release delay significantly. While the security updates are delayed only 25 days on average during monthly support, they are delayed 42 days and 62 days for the quarterly and biannual support types. For some of the models, the delay can go up to 300 days even though the device is still on the support list.

Other OEMs. Although Xiaomi started publishing monthly and quarterly supported devices in 2021 [83], it discontinued them after 2022. We found that their lists were never updated during this time. We found many inconsistencies in Xiaomi's support lists and we disregarded the results since they discontinued the publication of the support lists. Xiaomi started publishing the End-of-Support (EOS) product list, which is the list of devices not supported by Xiaomi anymore. However, since this list has also recently started, there is only limited data to perform our analysis.

Oppo categorizes its devices into two types of support: Monthly and Quarterly supported devices [49]. We performed a similar analysis as we did in the case of Samsung, calculating the monthly and quarterly periods for devices and examining the security updates received during those durations. We match the model using the firmware version provided in the security update. However, we found that the devices with monthly support did not receive any security updates during their time on the support lists. On the other hand, we found that 37 pairs of `A15`, `A73 5G`, and `A9` received some security updates during their quarterly supported duration. Yet, most of those devices received only three security updates, which restricts our ability to analyze the impact of support types on Oppo devices. This also suggests that support types do not have as significant an impact on Oppo devices as they do on Samsung devices.

> **Takeaway-3:** *Overall, our results indicate that while devices are on the support list, the timeliness and availability of security updates vary significantly for different support types. Moreover, our findings suggest that simply being on a support list does not guarantee the regular receipt of security updates in practice.*

B. Geolocation

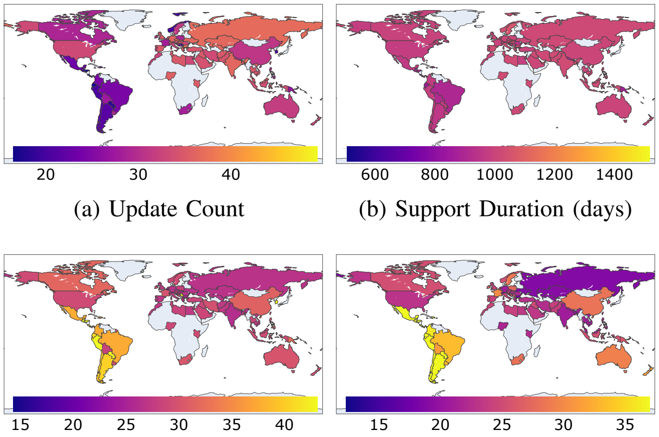
In this section, our goal is to analyze the impact of geolocation on the distribution of security updates. We identified the intended region for the security updates by using the following methodology: Security updates of Samsung devices are published per CSC-model pair. We use CSC to extract the country as well as the region via ISO definitions [6]. Xiaomi identifies 10 regions for their security updates. These regions include the Global and European Economic Area (EEA) or individual countries like China and India. For Oppo, we obtained the region from the URL that the security update info was published at and we obtained 35 unique countries. Finally, Google does not categorize its security updates based on the region.

Samsung. For Samsung, to minimize the impact of other factors like the support type, analyzed each support type separately. Figure 7 shows the heatmap of the security updates for monthly supported Samsung devices in all countries. The maps clearly demonstrate significant regional variances in terms of the number of monthly updates (Figure 7a), update frequency (Figure 7c), and release delay (Figure 7d), whereas the distribution for the support duration seems uniform to some degree across the regions (Figure 7b). We refer to Section A-A in the Appendix for the heatmaps of Samsung devices that are supported quarterly and biannually.

In this part, we grouped and sorted the countries in terms of the update count, support duration, update frequency, and release delay. We then selected the top five and bottom five countries for further detailed analysis. Table II presents the top and bottom five countries and their subregion for different support types. According to the results of the monthly support period, three of the top five countries receiving the most security updates are in Europe and the other two are in Central

TABLE II: Security updates received for different countries during monthly, quarterly, and biannually support type. We grouped and sorted the countries in terms of the update count, support duration, update frequency, and release delay. We then selected the top five and bottom five countries for further analysis.

		Monthly						Quarterly						Biannual			
Subregion	Country	Update Count	Support Duration	Update Freq	Release Delay	Subregion	Country	Update Count	Support Duration	Update Freq	Release Delay	Subregion	Country	Update Count	Support Duration	Update Freq	Release Delay
Western Europe	Luxembourg	39.0	1068.0	26.8	21.0	Southern Europe	Albania	15.0	645.0	40.3	40.0	Eastern Asia	Hong Kong	5.5	556.5	93.2	62.5
Eastern Europe	Russia	38.0	1053.0	27.2	20.0	Eastern Europe	Ukraine	12.0	628.5	53.0	36.0	Australia and New Zealand	Australia	5.5	461.5	81.0	69.5
Western Europe	Switzerland	38.0	1050.0	27.8	18.0	South-eastern Asia	Thailand	12.0	628.0	50.8	37.5	Southern Europe	Serbia	5.0	619.0	104.8	87.0
Central Asia	Uzbekistan	38.0	1043.0	27.8	18.0	South-eastern Asia	Malaysia	12.0	619.0	51.7	36.0	Southern Europe	Bosnia and Herzegovina	5.0	577.0	100.6	78.0
Southern Asia	India	37.5	1050.0	27.2	19.5	South-eastern Asia	Vietnam	12.0	617.0	50.1	35.0	Southern Asia	Bangladesh	5.0	568.0	93.1	88.0
Latin America and the Caribbean	Honduras	17.0	978.0	55.9	48.0	Northern Europe	Sweden	5.0	313.0	50.0	31.5	Western Europe	Belgium	1.0	-	-	81.0
Latin America and the Caribbean	Costa Rica	16.5	1041.5	56.1	46.5	Northern Europe	Norway	5.0	281.0	56.2	34.0	Latin America and the Caribbean	Costa Rica	1.0	-	-	77.5
Latin America and the Caribbean	Paraguay	16.0	972.0	60.1	48.0	Western Europe	Belgium	5.0	278.0	55.6	27.0	Western Asia	Israel	1.0	-	-	59.0
Latin America and the Caribbean	Ecuador	16.0	929.0	48.1	51.0	Sub-Saharan Africa	Mauritius	1.0	-	-	67.0	Northern Africa	Algeria	1.0	-	-	45.0
Latin America and the Caribbean	Jamaica	15.0	903.0	56.4	52.0	Sub-Saharan Africa	Zambia	1.0	-	-	67.0	Northern Europe	Sweden	1.0	-	-	16.0



(a) Update Count

(b) Support Duration (days)

(c) Update Frequency (days)

(d) Release Delay (days)

Fig. 7: Geolocation's impact on the distribution of security updates for monthly supported Samsung devices.

and Southern Asia. These top five countries receive monthly support for around three years with an update frequency of 26-28 days and a release delay of 18-21 days. On the other hand, all of the bottom five countries are in Latin America and the Caribbean. While devices in these countries receive monthly support, they received only 15-17 security updates despite having almost the same duration ($\sim$ 3 years) of support as the top countries. Similarly, these countries have a release delay of around 50 days, while we observed that the release delay of top five countries is around 20 days.

For the quarterly support period, while the top five countries receive 12-15 security updates, the countries in the bottom five receive three security updates on average. However, we observe that in the Sub-Saharan countries Mauritius and Zambia, the devices received a single security update with a delay of 67 days throughout their quarterly support. Similarly, the support duration of the bottom five countries is around 300 days, while the top five countries received support for more than 600 days. Similarly, the update frequency and release delay of the top five countries are either similar or better than those of the bottom five countries. During the biannual support period, while the devices from the top five receive five security updates, all of the bottom five receive a single security update. We observe that despite receiving a single security update, while Sweden's release delay is only 16 days, Belgium's delay is 81 days. Moreover, among the top five countries, the average support duration is generally around 550 days except for Australia, for which the duration is 461 days.

Overall, we observe that the impact of geolocation on update timeliness is more pronounced for devices on monthly support, followed by devices on quarterly support, and then devices on biannual support. Especially during the monthly support, there is a clear distinction in the number and timeliness of security updates received by devices in the top five countries, which are primarily European and one from Southern Asia, as compared to those in the bottom five countries. *We observe that the devices used in the top five countries receive two times more security updates, while the bottom five countries receive the security updates with three times longer delay.*

Other OEMs. The Xiaomi dataset includes 10 regions: China, Global, EEA, Russia, India, Turkey, Indonesia, Taiwan, Japan, and Singapore. On average, most of these regions receive between 2-4 security updates while Singapore receives the highest number of security updates with six security updates on average. Following Singapore, devices used in China receive an average of 4.5 security updates, indicating the tendency to provide more security updates in Asian regions. Additionally, the support duration for devices used in China is noticeably longer, at 274 days on average compared to an average of only 136 days in other regions. We do not observe any regional differences in update frequency and release delay.

The Oppo security update dataset includes 35 countries from three regions: 1) Africa & Middle East, 2) Asia Pacific, and 3) Europe. Among these three regions, Oppo devices used in Europe received nine security updates on average with a frequency of 68 days. However, the other two regions receive relatively fewer security updates (7-8 days) and less frequently (86-89 days). On the other hand, the average support duration and release delay of all the regions are similar with only slight differences. This trend also continues at the country level, where European countries like Italy and France receive the highest number of security updates together with the East Pacific countries like Japan and India with an average of 10 or more security updates. On the other hand, African countries like South Africa, Jordan, Egypt, and Nigeria receive around 3-5 security updates throughout the device's lifetime.

Takeaway-4: *In summary, variations in support across different regions and countries are observable among all OEMs. Samsung's update timeliness has regional influences, particularly noticeable during the monthly support phase. Meanwhile, for Oppo and Xiaomi, the disparities are less pronounced, with Oppo showing more uniformity across the regions, and Xiaomi revealing significant disparities only in the support duration metric.*

C. Device Type

In this section, we examine the impact of device types on the distribution of security updates.

Samsung. *We found that no Samsung tablet has received monthly support; instead, tablets are directly listed in the quarterly support list.* Wearables, on the other hand, are published in their own support list without a specified update frequency. There are 22 tablets that completed their quarterly support period and nine that completed their biannual support period while no wearable devices have yet completed their support period. Comparing tablets and phones during the quarterly and biannual support duration, we observe that smartphones stay longer in the support lists for both support durations. In particular, smartphones stay in the support list more than twice as long as tablets, with a total of 2202 days (1044 monthly + 597 quarterly + 561 biannual) versus 927 days (450 quarterly + 477 biannual) for tablets.

In addition to the duration in the support list, we also compared the security updates received by each device type. During the quarterly support period, the average update count for tablets is 12, compared to nine for smartphones. Tablets have 668 days of quarterly support and 276 days of biannual support on average whereas smartphones have 543 days of quarterly and 450 days of biannual support. These results indicate that tablets receive more security updates over a longer support duration during the quarterly support while smartphones receive more security updates during other support periods. This could be because tablets, which initially enter the support cycle with a quarterly support schedule, might be set up to receive more extensive update coverage from the outset.

Other OEMs. Xiaomi has 11 tablet models in our dataset that have received security updates. The models that received the most security updates are `Redmi Pad` and `Xiaomi Pad 5` with eight and seven security updates received respectively throughout their lifetime. The average of all metrics for Xiaomi tablets is very similar to those for smartphones, with only slight differences. In particular, tablets receive slightly more security updates on average, more frequently, but for a shorter support duration and more delay. On the other hand, while the software update webpages we used to download Oppo's security updates are not specific to smartphones, we found that Oppo has yet to publish any security updates for its tablets in any of the 35 countries. Google has only one tablet model, `Pixel C`, which exhibits the same support behavior as its smartphones, as demonstrated in Figure 4.

Takeaway-5: *In summary, device type influences Samsung's security update distribution, but not that of Google or Xiaomi. Samsung tablets do not receive monthly support, and smartphones remain on the support list considerably longer than tablets, suggesting the device type as a major factor impacting security updates.*

D. Carrier Association

Samsung. For this analysis, we created two categories (i.e., carrier-branded vs. non-carrier) based on the carrier CSCs, relying on Samsung's carrier association. The most common carriers in our dataset are Vodafone, T-Mobile, and Claro. On average, carrier-branded devices receive 29 monthly updates while non-carrier devices receive 32 security updates throughout their monthly support. There is only a slight difference (within 10%) between carrier-branded and non-carrier devices during the quarterly support period (9 and 10 updates, respectively) and no difference during the biannual support period (3 updates each). On the other hand, carrier-branded and non-carrier devices receive a similar duration of monthly support (∼992 days) and biannual support (∼350 days) while during the biannual support, non-carrier devices (523 days) receive longer support than carrier-branded devices (461 days). Lastly, the carrier devices experience more SPL release delay (29 days) than the non-carrier devices (26 days) during the monthly support.

Others. We found that neither Xiaomi nor Oppo specifies the carrier in their security updates. On the other hand, Google specified the carrier for 25% of updates (281 updates). Google's carrier definitions sometimes specify the exact carrier such as Verizon; however, sometimes they are described as "Verizon MVNOs" or "All carriers except TW". Using the given definitions, we do not observe any differences between the carriers regarding the security update distribution.

Takeaway-6: *Overall, across all OEMs, the security update behavior shows minimal variation between carrier-branded and non-carrier devices, indicating that the carrier's influence on these updates is limited.*

E. Partnership Agreements and Platform Solutions

In this section, we investigate the effect of partnership agreements and platform solutions on the distribution of security updates.

1) Android Enterprise Recommended (AER): AER is a Google-led program providing a list of devices and service providers that meet the given hardware and software requirements. Samsung has 60, Xiaomi has 46, Oppo has 18, and Google has 20 AER-certified devices [9]. Each device has a guaranteed date for the last security update and major OS upgrade.

Samsung. We first analyze the support list for AER-certified Samsung devices. We first analyze the support lists for the comparison of AER vs. non-AER devices. Out of 60 AER-certified devices, 49 devices appeared in the support lists and only seven of them completed their monthly support period. None of them so far have completed quarterly and biannual support types yet. The results show that AER devices stay on the monthly support list slightly longer than non-AER devices (i.e., 1072 days vs 1028 days). Moreover, we observed that AER-certified devices receive slightly more security updates, better duration, frequency, and delay performance during the monthly support compared to non-AER devices, aligning with our results from the support lists.

Others. For Xiaomi's 46 AER-certified devices, we found 82 corresponding pairs in our dataset. Of these 82 pairs, 70 pairs received security updates in the last three months. Among the remaining pairs, only two – the global distribution of `Mi A2 Lite` and `Mi A2` – have not received security updates in a year. Both devices' last guaranteed dates are aligned with the reported last support dates. Our analysis did not reveal any significant differences in security support behavior between AER-certified and non-AER Xiaomi devices. Oppo has 23 AER-certified devices with a guaranteed support date of March 2023 or later. We found that none of the 72 devices in our dataset are AER-certified. Consequently, we are unable to compare the impact of the AER certification on Oppo's update distribution. Finally, all Google devices carry AER certification. Therefore, all our analyses so far regarding Google devices apply to Google AER-certified devices.

2) Samsung Knox: Knox is a Samsung-led mobile device security program that ensures data security on Android devices via hardware-backed architecture. It applies to the selected devices listed in [57]. The platform for the devices with limited Knox support is called Android Others and the devices with no Knox compatibility are marked as Android Go [56]. In our support lists, 175 devices are marked as Knox, 25 devices are marked with Android Others, and 4 devices are marked as Android Go as their platforms. A comparison of support lists shows that there are no Android Others or Go devices that completed monthly support while there Knox-supported devices in all types of supports. The fact that there are no Android Other and Android Go devices that completed monthly support is a clear indication of the effectiveness of Android Knox programs. Moreover, during the quarterly period, we observed that there is no significant difference between Knox-supported and other devices in terms of the update count, support duration, update frequency, and release delay. In addition, Android Go devices receive only 108 days of biannual support, while Android Knox devices receive 372 days of biannual support on average. That is, Android Knox devices also receive longer biannual support than others.

Takeaway-7: *Overall, our findings indicate that while there may be small variations, the partnership agreements and the platform solutions are not a major factor within the same support type. However, they do have an impact on the support type a device is eligible for. This, in turn, affects the extent and quality of security support that a device will ultimately receive.*

VI. Key Issues and Exemplary Practices

Our research also revealed several key issues regarding the distribution of Android security updates and exemplary practices that can be adopted by OEMs to provide more transparency regarding their security support practices.

A. Key Issues

We have identified several key issues that OEMs could address promptly to enhance both the timeliness of security update distribution and the transparency of information provided to users.

Issue-1: Variations in Models' and Pairs' Support Behavior. Samsung, Xiaomi, and Google present their support lists using publicly known device names (e.g., `Samsung Galaxy S21`) [70], [83], [32] while Oppo includes specific models (e.g., `Find X2 (CPH2023)`) as well [49]. We have observed throughout this paper that each pair or model may have a different security update profile. One example is the variation in the support end date. We found that the support end date for pairs of `Galaxy S20 FE 5G` varies by more than two years. For example, the pair `SM-G781B/XEH` [64] used in Hungary received its last security update in October 2020, while the pair `SM-G781B/BGL` [65] used in Bulgaria received in March 2023, which is more than two years later. Not only the support end date, but these two pairs also have varying SPL levels and the last Android versions. Although the devices are generally known by their device name in the public eye, these results indicate each pair has a unique security update behavior. This highlights the need for unique identification and tracking of each model and pair of a device, as they may have distinct security update behaviors.

Issue-2: Discrepancies in Support Lists. The above example illustrates the distinct security update behaviors of different pairs. We also observed that some devices stay in the support lists despite stopping receiving any security updates. For instance, the device `Galaxy A7 (2018)` stayed on the biannual support list until "2022-11-0" [73]; however, the pair `SM-A750G/ALE` [58] stopped receiving security updates 1272 days before that date. Likewise, certain devices that appeared in the support lists have never received security updates or received a single security update. For example, `Galaxy Note FE` appeared in the quarterly and biannually support lists until the date of "2021-09-05" [73] but one of its pair `SM-N935F/CAM` [59] or `SM-N935F/KSA` [60] only received a single security update throughout its lifetime. While we excluded the devices that received no security updates to understand the overall characteristics of the support behavior, this highlights the need for more transparent and consistent data from OEMs. Comparable examples can be found with Oppo as well. For example, Oppo devices used in 16 countries with the models `Reno4`, `Reno4 5G`, `Reno4 Lite`, and `Reno4 F` models have not received any security updates since 2020. Overall, discrepancies in the support lists across the OEMs are noticeable.

Issue-3: Discrepancies in Partnership Agreements. Samsung provides the list of AER-certified devices with their guaranteed support date and guaranteed OS version. In the current list, AER-certified devices' guaranteed security updates are all a future date. However, we found that some of the models already stopped receiving security updates for a long time. Out of 5125 pairs of those AER-certified devices, 94% (4835) of them received security updates in the last two months. However, we found that 201 pairs have not received any security update in the last year, 58 pairs for two years, and 15 pairs have not received any security update in the last three years. Most of those pairs that have not received security updates in the last three years belong to Galaxy Note10 [61], Galaxy Note10+ [72], and Galaxy S10e [62]. One can verify the current AER status of these devices and their models in [57]. Likewise, two AER-certified pairs – global versions of Mi A2 Lite and Mi A2 – have not seen any security updates in the past year. This discrepancy between partnership commitments and actual security update rollouts further illustrates the inconsistencies within the security support landscape.

Issue-4: Misleading Announcements. In February 2021, Samsung announced "at least four years of security updates" for a list of devices [63], and in February 2022, they also announced "Four Generations of OS Upgrades" and "five years of security updates" for select devices [71]. The first announcement included 85 devices, in which we found a total of 8033 pairs in our dataset. Out of those pairs, we found that 343 pairs have not received any security updates in the last year, including some flagship devices like Galaxy S21 5G, Galaxy Note10, or Galaxy Note20. And, more than half of the devices did not receive the most recent security update yet. Similarly, the second announcement included 12 devices. We examined the security updates received for those devices. We found that Galaxy S21+ and Galaxy S21 Ultra used in Canada never received security updates after the date "2022-01-11", even though being on the list of supported devices in the announcement.

B. Exemplary Practices

We have also observed a number of exemplary practices already in use by some OEMs. If adopted more widely, these strategies could significantly enhance the overall efficiency and transparency of security updates within the Android ecosystem.

Practice-1: Guaranteed Support Date. Although OEMs might be publishing the list of devices that are currently supported, it can be challenging for users to determine the length of support for each device. Providing a guaranteed support date for each device would assist users in selecting devices that will continue to be supported for a desired period of time. While Motorola and Pixel currently implement this practice, their market share is relatively small. This is also recommended by the Federal Trade Commission (FTC) [22]. It would be advisable for other OEMs to adopt this approach to provide greater transparency and support for their customers.

Similarly, we discovered that the availability of updates depends on various factors that may be conflicting or unclear. The uncertainty is not resolved until the security update is actually released and received by the end user, which exposes users to risk. It is therefore essential for users to be aware of the security update schedule for the devices they plan to use to protect themselves from vulnerabilities.

Practice-2: End-of-Support Device List. Some OEMs like Motorola [40] and Xiaomi [83] release a list of devices that reached the end-of-support. This transparency allows users to easily determine whether their device will no longer receive any future security updates.

Practice-3: Model Support Lists. As observed throughout our analysis, the support behavior can significantly vary among different models. Hence, a more streamlined approach would be to present the support lists based on specific models rather than generic device names. This would provide users with a clear support schedule tailored to their specific model. Among all the OEMs we reviewed, only Oppo adopts this customer-centric approach in their support list announcements [49].

VII. Discussion and Limitations

In this section, we discuss the limitations of this work.

Samsung's Large Dataset vs. Other OEMs. There are several reasons why Samsung's dataset is vastly larger than those of Xiaomi, Oppo, and Google. First, Samsung has consistently held the largest market share and number of devices over the past decade, whereas Xiaomi and Oppo have only recently started to gain a substantial share of the market. Second, Samsung uniquely categorizes devices into model-CSC pairs. With approximately 314 CSC numbers, each model ends up generating around $\sim$300 security updates. Lastly, Samsung has consistently announced security updates via a dedicated webpage over the years, whereas other OEMs periodically change their announcement platforms, leading to potential missed updates in our data collection. For example, a notable limitation in our dataset is the absence of security update information for Oppo in China, the US, and the UK. This is due to these countries requiring specific device-related information to access the latest updates, which are not publicly available.

Active User Base. Devices not receiving security updates, even for a short period, expose their users to risks. We quantified this by calculating the accumulation of CVEs per device in Section IV-B. Although these devices pose a threat to their users, we lack information on the active user base for these devices. This data would be a valuable addition to our analysis and provide a more comprehensive understanding. To overcome this issue, we utilized popular devices from the support lists such as the Samsung Z Fold3 5G analyzed in Section IV-B or other sections in general. Though we lack data on an active user base data, our findings on supported devices provide insights for the potential durability of mobile devices, especially in the context of the recently-enacted Ecodesign directive in the EU [18].

Generalizibility to Smaller OEMs and Carriers. In this study, we mainly utilized two datasets from the OEMs: 1) support list snapshots, and 2) security updates history. Support list snapshots provide the anticipated support timeline for the devices while the security updates history provides the actual security updates that are made available for the end devices. Although some OEMs such as Vivo [80], LG [37], Motorola [40], Blackberry [17], Nokia [42] publishes the support lists, none of them publish a historical security update dataset that meets the requirements we used in Section III. For instance, Nokia does not specify any region or carrier [41]; OnePlus only releases the latest security updates [44]; Realme releases updates for Realme UI 1.0 only [53]; and Sony only released major OS upgrades [74].

On the other hand, US carriers like Verizon [79], AT&T [14], and T-Mobile [76] do not have a centralized website for security updates, i.e., they publish security updates for each device in device-specific URLs. The study in [35] collected carrier security updates from U.S. carriers and analyzed the delays introduced by these carriers This study can also be expanded to examine the international carriers providing software update schedules such as Vodafone Australia [15], Rogers [54] or Fido [31] used in Canada, Orange [50] used in Romania. Although the carrier impacts the delay, it is likely to have no impact on the schedule of the security updates after it is created by the OEM. We leave this as a future work.

Reasoning about the Results. One of the challenges we faced during this study was to identify the reasons behind certain findings. For example, if we found a specific country receives security updates late or occasionally misses updates, we are unable to deduce the reasoning behind this due to the lack of any public explanation provided by the OEMs. While we can technically speculate on factors like OEM priorities, policies, or implementation processes that might influence these practices, it is challenging to clearly identify and attribute these factors as only the OEMs can provide definitive answers. Our findings set the stage for future research to explore these practices and decisions and inform the scientific community about the issues.

VIII. Related Work

Our work builds upon and extends previous research on Android security updates.

Android Security Updates. Prior studies focused on different aspects of Android security. Possemato et al. [51] analyzed compliance and customization practices of Android OEMs and explored their effects on Android security. Farhang et al. [21] performed an empirical study of Android security bulletins from different OEMs. Farhang et al. [20] also conducted a large-scale study on Android CVEs where they examined the lifetime of CVEs. However, they do not perform an analysis at the OEM level. Wu et al. [82] analyzed Android system vulnerabilities and the patching behavior through code pattern analysis. Finally, the studies in [23], [36], [43], [55] focused on the app update behavior of Android users.

Rollout of Android Security Updates. Recent studies focused on the rollout of the Android security updates [87], [35], [34]. Zhang et al. [87] studied the delay during the propagation of Android kernel patches. Jones et al. [35] examined the Android security updates across different manufacturers, carriers, and end users to estimate the delay introduced by each. In addition, Hoe et al. [34] utilized Android firmware from 153 vendors to understand the timeliness and efficacy of security updates.

Our Differences. Owing to our collection of a large and representative dataset, our dataset, analysis, and results have unique aspects providing a more comprehensive and nuanced view of the issues surrounding Android security updates. This study reveals the impact of the factors like support type, geolocation, or device models (i.e., carrier type, device type, partnership agreements) on the rollout of Android security updates, in addition to the fragmentation issues studied in prior studies. Our study is the first to investigate the security posture of unpatched Android devices, while previous studies mostly used flagship devices with regular maintenance schedules. Finally, unlike proprietary user data in [35] and third-party firmware in [34], [87], we utilize official and publicly available security updates, ensuring our results are fully reproducible, more reliable, and serve as a valuable resource for future research.

IX. Conclusion

Using a dataset of 367K security updates, we were able to analyze the support behavior of Android devices used in 97 countries, associated with 109 carriers spanning from 2014 to 2023. This large and representative dataset allowed us to explore the broader Android ecosystem. We discovered significant variations in the number of security updates across regions and specific models, even within the same support type. Furthermore, for the first time in the literature, we quantified the risks associated with using unpatched Android devices and showed that the devices used during the unsupported duration may put users at significant risk for publicly known, remotely exploitable, and simple attacks that require no user interaction. This study suggests that the OEMs still have room for taking accountability of their security update practices, which can be achieved by publishing the support duration of all device models, and by maintaining the timeliness of their security updates. In addition, our work highlights the need for further research to understand and address the disparities in update provisioning.

Acknowledgment

This work was partially supported by the US National Science Foundation (Awards: 1663051, 2039606, 2219920), Cyber Florida, and Google's ASPIRE Program. The views expressed are those of the authors only, not of the funding agencies. We thank Sudhi Herle, Mihai Christodorescu, and Dave Kleidermacher of Android Security and Privacy (ASAP) at Google for their valuable feedback.

References

[1] Google android vulnerability statistics. https://www.cvedetails.com/product/19997/?q=Android, 2021. [Online; accessed 6-September-2021].

[2] https://www.reddit.com/r/GalaxyS7/comments/igmzx9/is_s7_no_longer_getting_quarterly_android/, 2023. [Online; accessed 19-June-2023].

[3] https://www.reddit.com/r/Android/comments/ubhp7f/samsung_galaxy_s22_may_security_update_already_out/, 2023. [Online; accessed 19-June-2023].

[4] https://www.reddit.com/r/GalaxyS21/comments/znc5kv/not_getting_security_update_on_s21/, 2023. [Online; accessed 19-June-2023].

[5] https://www.phonearena.com/news/update-late-for-pixel-6-pixel-7-t-mobile_id144825, 2023. [Online; accessed 19-June-2023].

[6] Iso-3166-countries-with-regional-codes. https://github.com/lukes/ISO-3166-Countries-with-Regional-Codes/blob/master/all/all.csv, 2023. [Online; accessed 10-Jan-2022].

[7] Jupyter notebook. https://jupyterbook.org/en/stable/intro.html, 2023. [Online; accessed 15-Nov-2023].

[8] List of samsung csc codes — samsung firmware csc codes. https://tsar3000.com/list-of-samsung-csc-codes-samsung-firmware-csc-codes, 2023. [Online; accessed 3-Jan-2022].

[9] Android. Google verified devices and services. https://www.android.com/enterprise/recommended/, 2023. [Online; accessed 3-Jan-2022].

[10] AOSP. Android 10 release notes. https://source.android.com/docs/setup/about/android-10-release, 2023. [Online; accessed 3-Jan-2022].

[11] AOSP. Android security bulletins. https://source.android.com/security/bulletin, 2023. [Online; accessed 5-June-2023].

[12] AOSP. Modular system components. https://source.android.com/docs/core/ota/modular-system, 2023. [Online; accessed 3-Jan-2022].

[13] A. O. S. P. (AOSP). Android security bulletins. https://source.android.com/docs/security/bulletin, 2023. [Online; accessed 16-Jan-2023].

[14] AT&T. At&t device support. https://www.att.com/device-support, 2023. [Online; accessed 3-Jan-2022].

[15] V. Australia. Software updates for devices. https://www.vodafone.com.au/support/device/software-updates, 2023. [Online; accessed 17-Jan-2023].

[16] I. Beer. Mind the gap. https://googleprojectzero.blogspot.com/2022/11/mind-the-gap.html, November 2022. [Online; accessed 23-June-2022].

[17] Blackberry. Blackberry product security incident response team. https://www.blackberry.com/us/en/services/blackberry-product-security-incident-response, 2023. [Online; accessed 10-Jan-2022].

[18] E. Commission. Designing mobile phones and tablets to be sustainable – ecodesign. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12797-Designing-mobile-phones-and-tablets-to-be-sustainable-ecodesign_en, 2023. [Online; accessed 18-September-2023].

[19] W. Enck, M. Ongtang, and P. McDaniel. Understanding android security. *IEEE Security & Privacy*, 7(1):50–57, 2009.

[20] S. Farhang, M. B. Kirdan, A. Laszka, and J. Grossklags. Hey google, what exactly do your security patches tell us? a large-scale empirical study on android patched vulnerabilities. *arXiv preprint arXiv:1905.09352*, 2019.

[21] S. Farhang, M. B. Kirdan, A. Laszka, and J. Grossklags. An empirical study of android security bulletins in different vendors. In *Proceedings of The Web Conference 2020*, pages 3063–3069, 2020.

[22] F. T. C. (FTC). Ftc recommends steps to improve mobile device security update practices. https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update-practices, 2023. [Online; accessed 3-Jan-2022].

[23] J. Gajrani, M. Tripathi, V. Laxmi, G. Somani, A. Zemmari, and M. S. Gaur. Vulvet: Vetting of vulnerabilities in android apps to thwart exploitation. *Digital Threats: Research and Practice*, 1(2):1–25, 2020.

[24] Google. Android and google devices security reward program rules. https://bughunters.google.com/about/rules/6171833274204160/android-and-google-devices-security-reward-program-rules, 2021. [Online; accessed 9-Jan-2023].

[25] Google. Compatibility test suite. https://source.android.com/docs/compatibility/cts, 2021. [Online; accessed 9-Jan-2023].

[26] Google. Pixel update bulletins. https://source.android.com/docs/security/bulletin/pixel, 2021. [Online; accessed 9-Jan-2023].

[27] Google. Security updates and resources. https://source.android.com/docs/security/overview/updates-resources, 2021. [Online; accessed 9-Jan-2023].

[28] Google. Android updates on nexus devices. https://support.google.com/nexus/answer/11227897, 2023. [Online; accessed 7-Apr-2023].

[29] Google. Codenames, tags, and build numbers. https://source.android.com/docs/setup/about/build-numbers, 2023. [Online; accessed 2-Apr-2023].

[30] Google. Factory images for nexus and pixel devices. https://developers.google.com/android/images, 2023. [Online; accessed 2-Apr-2023].

[31] Google. Get help from your device manufacturer & mobile carrier. https://forums.fido.ca/t5/Phones-and-Devices/OS-Upgrade-Schedule/ta-p/185669, 2023. [Online; accessed 10-Jan-2023].

[32] Google. Learn when you'll get software updates on google pixel phones. https://support.google.com/pixelphone/answer/4457705, 2023. [Online; accessed 7-Apr-2023].

[33] Hackernews. Unpatched strandhogg android vulnerability actively exploited in the wild. https://thehackernews.com/2019/12/strandhogg-android-vulnerability.html, 2019. [Online; accessed 20-June-2023].

[34] Q. Hou, W. Diao, Y. Wang, X. Liu, S. Liu, L. Ying, S. Guo, Y. Li, M. Nie, and H. Duan. Large-scale security measurements on the android firmware ecosystem. In *International Conference on Software Engineering (ICSE'22)*, 2022.

[35] K. R. Jones, T.-F. Yen, S. C. Sundaramurthy, and A. G. Bardas. Deploying android security updates: an extensive study involving manufacturers, carriers, and end users. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 551–567, 2020.

[36] A. Kalysch, J. Schilling, and T. Müller. On the evolution of security issues in android app versions. In *International Conference on Applied Cryptography and Network Security*, pages 523–541. Springer, 2020.

[37] LG. Lg mobile security bulletins. https://lgsecurity.lge.com/bulletins/mobile#updateDetails, 2023. [Online; accessed 10-Jan-2022].

[38] W. Machine. Internet archive. https://archive.org/, 2023. [Online; accessed 3-Jan-2022].

[39] W. Machine. Introduction to samsung security updates. https://web.archive.org/web/20230620061009/https://security.samsungmobile.com/workScope.smsb, 2023. [Online; accessed 3-Apr-2023].

[40] Motorola. Android security updates. https://motorola-global-portal.custhelp.com/app/software-security-update/g_id/7112, 2023. [Online; accessed 10-Jan-2022].

[41] Nokia. Nokia smartphone security maintenance release summary. https://www.nokia.com/phones/en_int/security-updates, 2023. [Online; accessed 3-Apr-2023].

[42] Nokia. Will my nokia smartphone receive security updates? https://www.nokia.com/phones/en_us/support/topics/software-and-updates/will-my-nokia-smartphone-receive-security-updates, 2023. [Online; accessed 10-Jan-2022].

[43] E. Novak and C. Marchini. Android app update timing: A measurement study. In *2019 20th IEEE International Conference on Mobile Data Management (MDM)*, pages 551–556. IEEE, 2019.

[44] Oneplus. Oneplus smartphone software update. https://service.oneplus.com/us/search/search-detail?id=2096229, 2023. [Online; accessed 28-Jan-2022].

[45] OPPO. Oppo a11k firmware updates. https://support.oppo.com/in/software-update/software-download/?m=A11k, 2023. [Online; accessed 2-Apr-2023].

[46] Oppo. Oppo pembaruan firmware reno4 lite. https://support.oppo.com/id/software-update/software-download/?m=Reno4%20Lite, 2023. [Online; accessed 23-June-2022].

[47] Oppo. Oppo reno4 f firmware updates. https://support.oppo.com/kz/software-update/software-download/?m=Reno4%20F, 2023. [Online; accessed 23-June-2022].

[48] Oppo. Oppo reno4 firmware updates. https://support.oppo.com/ng/software-update/software-download/?m=Reno4, 2023. [Online; accessed 23-June-2022].

[49] Oppo. Security advisories. https://security.oppo.com/en/mend, 2023. [Online; accessed 10-Jan-2022].

[50] Orange. The first security update for samsung phones in 2020 solves over 50 vulnerabilities... the first security update for samsung phones in 2020 solves over 50 security vulnerabilities. https://www.orange.ro/info/gadgets/article/2115813, 2023. [Online; accessed 17-Jan-2023].

[51] A. Possemato, S. Aonzo, D. Balzarotti, and Y. Fratantonio. Trust, but verify: A longitudinal analysis of android oem compliance and customization. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 87–102. IEEE, 2021.

[52] S. Ranger. Google android vulnerability statistics. https://www.zdnet.com/article/android-security-warning-one-billion-devices-no-longer-getting-updates/, 2020. [Online; accessed 6-September-2021].

[53] Realme. Software&driver update. https://www.realme.com/in/support/software-update, 2023. [Online; accessed 28-Jan-2022].

[54] Roger. Os upgrade schedule. https://communityforums.rogers.com/t5/OS-Upgrades/OS-Upgrade-Schedule/td-p/354931, 2023. [Online; accessed 17-Jan-2023].

[55] J. P. Rula, P. Richter, G. Smaragdakis, and A. Berger. Who's left behind? measuring adoption of application updates at scale. In *Proceedings of the ACM Internet Measurement Conference*, pages 710–723, 2020.

[56] Samsung. About secured by knox, android - others and android go devices. https://docs.samsungknox.com/admin/fundamentals/faqs/kba-349-about-android-others-android-go-devices.htm, 2023. [Online; accessed 3-Jan-2022].

[57] Samsung. Devices secured by knox. https://www.samsungknox.com/en/knox-platform/supported-devices, 2023. [Online; accessed 3-Jan-2022].

[58] Samsung. Galaxy a7 (sm-a750g). https://doc.samsungmobile.com/SM-A750G/ALE/doc.html, 2023. [Online; accessed 18-Jan-2023].

[59] Samsung. Galaxy a7 (sm-a750g). https://doc.samsungmobile.com/SM-N935F/CAM/doc.html, 2023. [Online; accessed 18-Jan-2023].

[60] Samsung. Galaxy a7 (sm-a750g). https://doc.samsungmobile.com/SM-N935F/KSA/doc.html, 2023. [Online; accessed 18-Jan-2023].

[61] Samsung. Galaxy note10 (sm-n970f). https://doc.samsungmobile.com/SM-N970F/ORO/doc.html, 2023. [Online; accessed 18-Jan-2023].

[62] Samsung. Galaxy note10 (sm-n970f). https://doc.samsungmobile.com/SM-N970F/PCW/doc.html, 2023. [Online; accessed 18-Jan-2023].

[63] Samsung. Galaxy products launched since 2019, including the z, s, note, a, m, xcover and tab series, will now receive at least four years of security updates. https://news.samsung.com/global/samsung-takes-galaxy-security-to-the-next-level-by-extending-updates, 2023. [Online; accessed 16-Jan-2023].

[64] Samsung. Galaxy s20 fe 5g (sm-g781b). https://doc.samsungmobile.com/SM-G781B/XEH/doc.html, 2023. [Online; accessed 24-Jun-2023].

[65] Samsung. Galaxy s20 fe 5g (sm-g781b). https://doc.samsungmobile.com/SM-G781B/BGL/doc.html, 2023. [Online; accessed 24-Jun-2023].

[66] Samsung. Galaxy z fold3 5g (sm-f926u1). https://doc.samsungmobile.com/SM-F926U1/TMB/doc.html, 2023. [Online; accessed 23-June-2022].

[67] Samsung. Galaxy z fold3 5g (sm-f926u1). https://doc.samsungmobile.com/SM-F926U1/TMK/doc.html, 2023. [Online; accessed 23-June-2022].

[68] Samsung. Galaxy z fold3 5g (sm-f926u1). https://doc.samsungmobile.com/SM-F926U1/XAA/doc.html, 2023. [Online; accessed 23-June-2022].

[69] Samsung. Galaxy z fold3 5g (sm-f926u1). https://doc.samsungmobile.com/SM-F926U1/XAG/doc.html, 2023. [Online; accessed 23-June-2022].

[70] Samsung. Introduction to samsung security updates. https://security.samsungmobile.com/workScope.smsb, 2023. [Online; accessed 3-Jan-2022].

[71] Samsung. Samsung sets the new standard with four generations of os upgrades to ensure the most up-to-date and more secure galaxy experience. https://news.samsung.com/global/samsung-sets-the-new-standard-with-four-generations-of-os-upgrades-to-ensure-the-most-up-to-date-and-more-secure-galaxy-experience, 2023. [Online; accessed 16-Jan-2023].

[72] Samsung. Sm-n975f. https://doc.samsungmobile.com/SM-N975F/ORO/doc.html, 2023. [Online; accessed 18-Jan-2023].

[73] W. M. (Samsung). Security updates. https://web.archive.org/web/20221104053955/https://security.samsungmobile.com/workScope.smsb, 2023. [Online; accessed 18-Jan-2023].

[74] Sony. Latest updates. https://developer.sony.com/open-source/aosp-on-xperia-open-devices/latest-updates, 2023. [Online; accessed 28-Jan-2022].

[75] Statcounter. Mobile vendor market share worldwide. https://gs.statcounter.com/vendor-market-share/mobile/worldwide, 2023. [Online; accessed 3-Jan-2022].

[76] T-Mobile. Wireless t-mobile support. https://www.t-mobile.com/support/, 2023. [Online; accessed 3-Jan-2022].

[77] G. S. Tuncay, S. Demetriou, K. Ganju, and C. A. Gunter. Resolving the predicament of android custom permissions. In *NDSS*, 2018.

[78] G. S. Tuncay, J. Qian, and C. A. Gunter. See no evil: phishing for permissions with false transparency. In *USENIX Security*, 2020.

[79] Verizon. Samsung galaxy s22 ultra software update. https://www.verizon.com/support/samsung-galaxy-s22-ultra-update/, 2023. [Online; accessed 3-Jan-2022].

[80] Vivo. Android security advisories. https://www.vivo.com/en/security, 2023. [Online; accessed 10-Jan-2022].

[81] S. Weigand. Api bug in oauth dev tool opened websites, apps to account hijacking. https://www.scmagazine.com/news/api-bug-oauth-dev-tool-hijacking, 2023. [Online; accessed 18-September-2023].

[82] D. Wu, D. Gao, E. K. Cheng, Y. Cao, J. Jiang, and R. H. Deng. Towards understanding android system vulnerabilities: techniques and insights. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 295–306, 2019.

[83] Xiaomi. Security updates for smartphones. https://trust.mi.com/misrc/updates/phone?tab=policy, 2023. [Online; accessed 10-Jan-2022].

[84] Xiaomi. Xiaomi official api. https://sgp-api.buy.mi.com/bbs/api/global/phone/getlinepackagelist, 2023. [Online; accessed 23-June-2022].

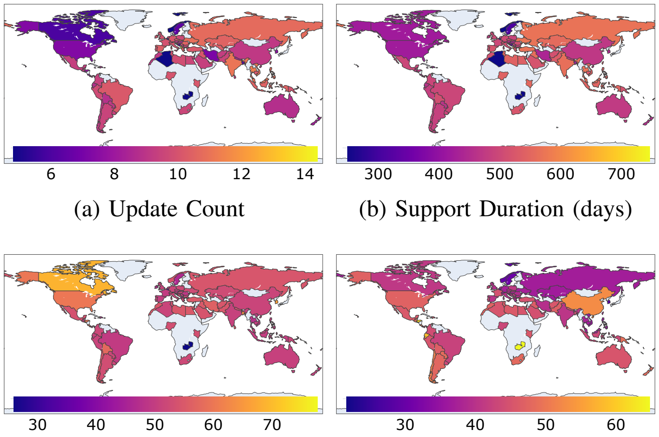
[85] xiaomifirmwareupdater.com. Miui updates tracker v3. https://github.com/XiaomiFirmwareUpdater/miui-updates-tracker, 2023. [Online; accessed 3-Apr-2023].

[86] XiaomiWiki.github.io. Regional names of xiaomi devices. https://github.com/XiaomiWiki/XiaomiWiki.github.io/blob/master/wiki/Regional_names_of_Xiaomi_devices.md, 2023. [Online; accessed 3-Apr-2023].

[87] Z. Zhang, H. Zhang, Z. Qian, and B. Lau. An investigation of the android kernel patch ecosystem. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3649–3666, 2021.

Appendix A
More on Geolocation Analysis

A. *Quarterly and Biannual Support Geolocation Analysis*



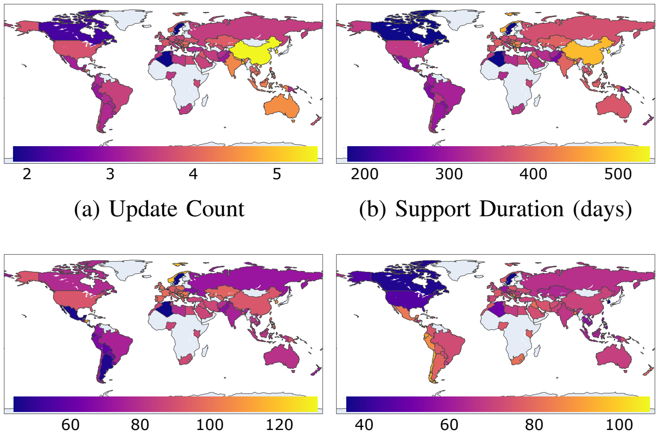
(a) Update Count

(b) Support Duration (days)

(c) Update Frequency (days)

(d) Release Delay (days)

Fig. 8: Distribution of security updates for quarterly supported Samsung devices.



(a) Update Count

(b) Support Duration (days)

(c) Update Frequency (days)

(d) Release Delay (days)

Fig. 9: Distribution of security updates for biannually supported Samsung devices.

Similar to the monthly support type, geolocation also impacts the quarterly and biannually support types. However, unlike the unaffected monthly support, geolocation does influence the duration of the quarterly and biannual support, as shown in Figure 8 and 9. Furthermore, regional performance differs across support types. For example, while the Northern Americas and European countries were among the best performers and Latin America and the Caribbean were the worst performers, the devices used in those regions have the same performance for quarterly and biannually support types.

Appendix B
Artifact Appendix

This section contains the mandatory artifact appendix required for the NDSS 2024 artifact evaluation.

A. Description & Requirements

This section lists all the information necessary to recreate the experimental setup we used to run our artifact.

1) How to access: The complete artifact can be found both at https://github.com/cslfiu/Android-Security-Updates and https://zenodo.org/doi/10.5281/zenodo.10139526. Please use the first link for the most up-to-date version, and the second link is for permanent storage.

2) Hardware dependencies: "None."

3) Software dependencies:

- Jupyter Notebook [7]
- Python Modules: `pandas`, `numpy`, `PyYAML`(>=5.4), `pycountry`, `matplotlib`, `plotly`, `tqdm`, `openpyxl`, `kaleido`

4) Benchmarks: "None."

B. Artifact Installation & Configuration

The artifact consists of two parts. In the first part, we explain the details of data collection and preprocessing. This part can be reproduced by following the same steps and crawling the data from the same sources. All data is collected from official and public sources. We have shared the full details of the data collection and preprocessing in the README of the repository. The second part of the experiments starts with the collected data from the first part. For full reproducibility, we also share the data collected during the first step under the 'Data' folder. One can start from the second step to reproduce the results in the paper.

C. Major Claims/Findings

Major claims/findings (Cx) in our paper are as follows:

- (C1): Google provides regular monthly security updates throughout the lifetime of an Android device while Samsung's security update frequency varies, depending on factors such as the support type, geolocation, device type, and others. Furthermore, Oppo and Xiaomi offer relatively fewer security updates for a relatively shorter duration.
- (C2) During the unsupported period, (unpatched) devices continue receiving critical, remotely exploitable CVEs that do not require user interaction. These CVEs tend to arise immediately after the end of support and taper off after two years.
- (C3) For devices on the support list, the timeliness and availability of security updates significantly vary across different support types.
- (C4) Variations in support across different regions and countries are observable among all OEMs.
- (C5) Device type influences Samsung's security update distribution, but not that of Google or Xiaomi. Samsung tablets do not receive monthly support, and smartphones remain on the support list longer than tablets.
- (C6) Security update behavior shows minimal variation between carrier-branded and non-carrier devices across all OEMs.
- (C7) The partnership agreements and the platform solutions are not major factors within the same support type. However, they do have an impact on the support type a device is eligible for.
- (C8) This study reveals several key issues, including variations in the support behavior of device models and pairs, discrepancies in support lists, discrepancies in partnership agreements, and instances of misleading announcements.

D. Evaluation

Our analysis consists of five sets of experiments. To verify these numerical results, one can follow the corresponding sections in the paper and run the code as described. This will allow you to cross-check the results presented in the paper with those you obtain. Below are the detailed steps for each experiment.

1) Experiment (E1): [Support List Analysis] [5 compute-minutes]: Analyzing OEM-provided support lists to extract device support timelines.

[How to] Load '`Code/1-Support-Lists.ipynb`' in Jupyter Notebook.

[Preparation] Ensure all required Python packages are installed.

[Execution] Run all cells in order.

[Results] The historical support lists for individual devices can be verified from their sources in Wayback Machine [70], [49], [83], [32]. The extracted support timelines from the support lists are used throughout the paper such as the support duration in Section IV-A, the support type analysis in Section V-A, and device type analysis in Section V-C.

2) Experiment (E2): [Supported Period Analysis] [8 compute-minutes]: Analyzing the security support behavior during the supported period.

[How to] Open '`Code/2-Supported-Period.ipynb`' in Jupyter Notebook.

[Preparation] Ensure all required Python packages are installed.

[Execution] Run all cells in order.

[Results] The dataset statistics are reported in Section III-A and the results of the supported period analysis are given in Section IV-A of the paper. Similarly, Figures 3 and 4 in the paper can be cross-referenced during this experiment. The claim C1 can be verified with the results in E1.

3) Experiment (E3): [Unpatched Period Analysis] [30 compute-minutes]: Analyzing the devices during an unsupported period to quantify the risk of using unpatched Android devices.

[How to] Access '`Code/3-Unpatched-Analysis.ipynb`' in Jupyter Notebook.

[Preparation] Ensure all required Python packages are installed. Also, download the CVE information via the provided script (“`download_cve.s`”). Make sure to run E2 before E3 since the last security update dates and last OS version information will be used here.

[Execution] Run all cells in order.

[Results] The results of unpatched device analysis are given in Section IV-B of the paper. Additionally, Figure 5 in the paper can be cross-referenced during this experiment. The claim C2 can be verified with the results in E3.

4) Experiment (E4): [Impacting Factor Analysis] [10 compute-minutes]: Analyzing the impacting factors on the availability and timeline of security updates by OEMs.

[How to] Open the Jupyter Notebook for E1 (‘`4-Factor-Analysis.ipynb`’).

[Preparation] Ensure all required Python packages are installed. Make sure to run E1 before E4 since the support types extracted from support lists will be used for the analysis here.

[Execution] Run all cells in order.

[Results] The results for the impacting factor analysis are in Section V of the paper. Figures 6 and 7 as well as Table II can be reproduced via this experiment. The claims C3, C4, C5, C6, and C7 also can be verified with the results in E4.

5) Experiment (E5): [Key Issues Analysis] [20 compute-minutes]: Analyzing the key issues such as inconsistency examples or discrepancies in AER-certified devices.

[How to] Open ‘`5-Key-Issues.ipynb`’ in Jupyter Notebook.

[Preparation] Ensure all required Python packages are installed. Make sure to run E1 before E5 as we are analyzing the consistency of support lists.

[Execution] Run all cells in order.

[Results] The results of the analysis of the key issues are given in Section VI of the paper. The key issues we found in the paper in Section VI and further issues can be re-produced via this experiment. The claim C8 can be verified with the results here.

E. Customization

Updating and Re-running the Data: As we generally provided statistical information regarding our dataset in the paper, one can further inspect the individual results if they desire. For example, while we can only report average values, one can plot the distribution graphs and check the exact values further. Similarly, for a more up-to-date perspective, one can re-run the unpatched analysis considering the CVEs published after our paper’s publications to identify other patterns.