

**Vulnerability, Where Art Thou?** An Investigation of Vulnerability Management in Android Smartphone Chipsets

Daniel Klischies, Philipp Mackensen, Veelasha Moonsamy





## Smartphone security: Multi-layered complexity



Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets





## Smartphone security: Multi-layered complexity



Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets





# Smartphone security: Multi-layered complexity

## **Open questions:**

- Do different chipsets share vulnerabilities?
- Who discovers chipset vulnerabilities?
- What are typical timeframes until vulnerabilities are mitigated?

And many more



Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets





## Components

**Application processor** 

Supplied by:

Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets



### Smartphone manufacturers





## Components



### Supplied by:

Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

Android Vision DSP GPU

### Smartphone manufacturers





## Components



### Supplied by:

Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

### Smartphone manufacturers





## Components



### Supplied by:

Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

### Smartphone manufacturers



RUHR UNIVERSITÄT BOCHUM





RUB

## Components



Supplied by:

Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

### Smartphone manufacturers



RUHR UNIVERSITÄT BOCHUM



RUB

**Vulnerability** introduction



### Chipset manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets









Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets









Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets





### Chipset manufacturers

















## Chipset vulnerability lifecycle **Vulnerability Vulnerability** introduction discovery Drivers Analyze Firmware Chipset **Researchers** manufacturers

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets



### → Challenge: Information is scattered across websites of involved companies







# Our knowledge base



![](_page_14_Figure_4.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_14_Picture_6.jpeg)

![](_page_14_Picture_8.jpeg)

# Our knowledge base

![](_page_15_Figure_1.jpeg)

![](_page_15_Picture_4.jpeg)

Chipsets.org Vulnerabilitie

### Tracking 3676 chipset vulnerabilities across 6866 different smartphone models.

What is this about? Every smartphone contains a chipset, enabling functionality such as calls, data connectivity, Bluetooth and WiFi communication, digital image processing and more. Detecting and addressing chipset vulnerabilities is crucial for optimal smartphone security. However, information on these vulnerabilities is scattered across chipset manufacturers' websites, AOSP's Security Bulletins, and OEM websites. Our website consolidates this data for a unified and accessible view.

![](_page_15_Figure_9.jpeg)

Our data provides a holistic overview on each phase of the vulnerability lifecycle.

### 斑 Vulnerability Introduction

Each new chipset release brings exciting features, yet often inherits vulnerabilities from previous generations.

### In each new chipset generation.

ና 93 %

of all vulnerabilities are inherhited from previous chipset generations

**∻ 7%** 

of all vulnerabilities occur in this chipset generation for the first time

### https://chipsets.org

![](_page_15_Picture_20.jpeg)

RUHR UNIVERSITÄT BOCHUM

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_15_Picture_24.jpeg)

![](_page_15_Picture_25.jpeg)

# Vulnerability introduction

![](_page_16_Figure_1.jpeg)

![](_page_16_Picture_4.jpeg)

### Current chipset model

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_16_Picture_7.jpeg)

![](_page_16_Picture_9.jpeg)

![](_page_17_Figure_1.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_17_Picture_5.jpeg)

![](_page_17_Picture_6.jpeg)

![](_page_17_Picture_7.jpeg)

![](_page_18_Figure_1.jpeg)

## **Takeaways**:

- Analyzing legacy features still yields new vulnerabilities
- A lot of code is **shared** between chipset models
  - Requires time consuming assessment which models include vulnerable code

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_18_Picture_11.jpeg)

![](_page_18_Picture_13.jpeg)

# Vulnerability discovery

## Who discovers most vulnerabilities post release (2023)?

![](_page_19_Figure_2.jpeg)

![](_page_19_Picture_5.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_19_Picture_8.jpeg)

![](_page_19_Picture_9.jpeg)

![](_page_19_Picture_10.jpeg)

![](_page_19_Picture_11.jpeg)

# Vulnerability discovery

## Who discovers most vulnerabilities post release (2023)?

![](_page_20_Figure_2.jpeg)

## **Takeaways:**

- Generally high reliance on external researchers
- Disclosure processes for external researchers exist & reports are taken seriously

![](_page_20_Picture_8.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_20_Picture_12.jpeg)

![](_page_20_Picture_14.jpeg)

![](_page_20_Picture_15.jpeg)

# Patch & Update timeline

![](_page_21_Figure_1.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_21_Picture_5.jpeg)

![](_page_21_Picture_7.jpeg)

# Patch & Update timeline

![](_page_22_Figure_1.jpeg)

![](_page_22_Picture_5.jpeg)

![](_page_22_Picture_6.jpeg)

![](_page_22_Picture_7.jpeg)

# Patch & Update timeline

## **Takeaways**:

- Updates are not well-coordinated across different phone models
- 90 day coordinated disclosure period is almost never adhered to
- → Patch development and update packaging both exceed 90 days frequently

95% of vulnerabilities

![](_page_23_Picture_7.jpeg)

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_23_Figure_10.jpeg)

![](_page_23_Picture_11.jpeg)

![](_page_23_Picture_13.jpeg)

## Additional use cases

![](_page_24_Picture_1.jpeg)

## Identify trends and avenues for future research

 $\rightarrow$  Which components yield the most severe vulnerabilities?  $\rightarrow$  Where do we see few vulnerabilities?

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

![](_page_24_Picture_8.jpeg)

![](_page_24_Picture_10.jpeg)

## Additional use cases

![](_page_25_Picture_1.jpeg)

## Identify trends and avenues for future research

- $\rightarrow$  Where do we see few vulnerabilities?

![](_page_25_Figure_5.jpeg)

## Make an informed selection of evaluation devices

Klischies et al.: Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

 $\rightarrow$  Which components yield the most severe vulnerabilities?

 $\rightarrow$  Many chipsets have almost the same set of vulnerabilities  $\rightarrow$  We offer a tool to estimate and select diverse sets of phone models

![](_page_25_Picture_12.jpeg)

![](_page_25_Picture_14.jpeg)

## Additional use cases

![](_page_26_Picture_1.jpeg)

Identify trends and avenues for future research

 $\rightarrow$  Which components yield the most severe vulnerabilities?  $\rightarrow$  Where do we see few vulnerabilities?

![](_page_26_Picture_4.jpeg)

Make an informed selection of evaluation devices  $\rightarrow$  Many chipsets have almost the same set of vulnerabilities  $\rightarrow$  We offer a tool to estimate and select diverse sets of phone models

![](_page_26_Picture_6.jpeg)

## Determine how widespread a recently found vulnerability is $\rightarrow$ List all chipsets <u>and</u> smartphones affected by a vulnerability

![](_page_26_Picture_13.jpeg)

![](_page_26_Picture_14.jpeg)

![](_page_26_Picture_16.jpeg)

![](_page_27_Picture_0.jpeg)

Chipsets.org Devices - Chipsets - Vulnerabilities -					Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets Daniel Klischies Man Linversity Bochum daniel Klischies Man Choment Schum Man Chipsets Man Chipsets	
Tracking 3676 chipset vulnerabilities across 6 different smartphone models.					Advance—Valuershillites in hadroid martphone chipsets have evere consequences, ar occut real-world attack [1] have dome strate did nat devarative can levery submrabilities to be con- trading impact devarative can levery submrabilities to be con- trading impact of neural probability of the strategies of the world of the strategies of neural probability of the strategies of the strategies of the strategies of the strategies	
	What is this about?	Every smartphone contains a cl communication, digital image p optimal smartphone security. H websites, AOSP's Security Bulle accessible view.	hipset, enabling functionalit rocessing and more. Detec owever, information on the titns, and OEM websites. Or	y such as ting and a se vulnerat ur website	generations. Furthermore, we demonstrate that the commosily accepted 40-bits preparability thermality disclosure period is affects hundreds to thousands of different sametyhane models, for which update availability is as we show, after unchar- ter harshy datayed. Lerrarging the new insights gained from ethopies manufactures can implement to improve the security positive of their products. At the same time, our knowledge has evaluations on simplement discourse wavenues for future research. IN INTRODUCTION Sametphones play an integral part of our daily lives and are emranted with affect-critical tasks, such as emergency calls and safegrating of ourse? coefficiential information. Most sumptiones parts of the source of the source of the source sametphones run a version of Android, which is the most have of 0.705 k. It is this of outnow innovations to maintain	browsing history, contact lists and location data from com- promised phones, and badyood flowly, vulnerabilities cooperation of the vicinity, service provider. To minimize the risk of being compounding, and the service provider. To minimize the service provider. To minimize the risk of being compounding, Amerya Jung Hang, and your devices." However, this recommendation assumes the devices of the service provides the service of the service service of the service provides of the service of the service of the service of the service of the service of the devices. If the service the service of the service of the form the chipset, rather than the device. Chipset processors are closely intertwined with their soft- ware, consisting of firmware, which mus on them, and the drivers that crastene therefores to the Androld OS. Chipset processor are indevice the service of the service of the service theory. I. (c) dright high-physical dimensional dimensional dimensional as a part of the Android Open Source Project (AOSP), This means that the CAN need to contingue to support and provide
() Vulnerabilities	Explore trends	Phone models	Show all	စ္မ်ို ပ၊	the security of Android smartphones by proactively identify- ing particularly vulnerable components as well as ensuring timely updates after a vulnerability has been discovered. An	updateo immware and arvers to OLEMS over the intellife or a chipset, in particular, to militigate security vulnerabilities. The primary goal when dealing with such vulnerabilities is to minimize the length of the winderability lifey-clck, i.e., the overall time frame a vulnerability is exploitable, by employing successful vulnerability management across the supply chain.
3676		6866 ② Chipsets	Show all	Phone m Samsung Samsung	Network and Distributed System Security (NDSS) Symposium 2025 214 (Hungy 2025; 200 June C.A. USA SINS (FORCE) 215 (1997) SINS (FORCE) 215 (1997) https://dx.doi.org/10.147220sbs.2025.241161 www.adas-symposium.org.	For smarphone chiptes, this time frame is divided into four plases: (1) the introduction of a vulnerability, (ii) its eventual discovery, (iii) the development of a patch removing the vulnerability by the CM, and (iv) packaging of the patch
	~	437 each affect	ted by 137 vulnerabilities (avg.)	Samsung Ga	ayy Tab AR 10.5	

In the paper & on https://chipsets.org: What are the most affected components? Differences between firmware and drivers Comparison to other ecosystems

. . .

![](_page_27_Picture_6.jpeg)

![](_page_27_Picture_8.jpeg)

![](_page_27_Picture_9.jpeg)

![](_page_27_Picture_10.jpeg)

![](_page_27_Picture_11.jpeg)