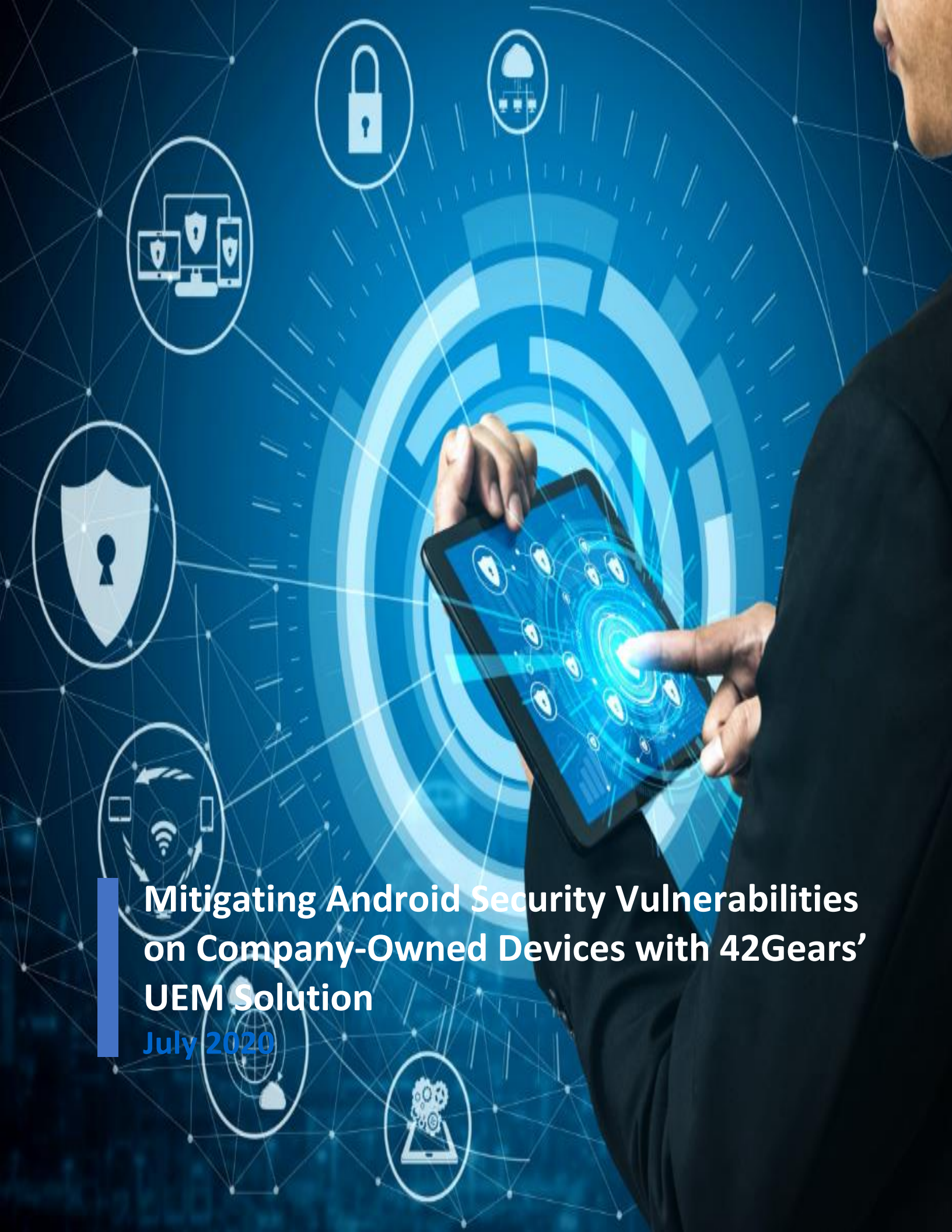

Mitigating Android Security Vulnerabilities on Company-Owned Devices with 42Gears' UEM Solution

July 2020

Table of Content

Executive Summary

42Gears provides comprehensive security for all Android devices including rugged devices through its robust and reliable UEM solution. The solution helps organizations protect and secure their mobile devices against all possible threats and vulnerabilities by offering comprehensive features such as Kiosk Mode, Network Policy, Security Policy and OS patch management. Further, the solution is capable of mitigating risks of malware attacks via phishing email, malicious apps, unknown networks and more. Our MTD provides an extra layer of security which keeps checking threat factors and helps admins in taking remedial actions in real time.

Overview

Android smartphones and tablets have gained popularity among businesses around the world, thanks to the wide range of business applications they support. **According to an IDC survey, Android devices comprised 78 percent of business device shipments in 2018[1]. The survey also predicted that the Android rugged devices market would grow by 23 percent by 2023.**

However, as the use of various kinds of Android devices (point of sale machines, rugged devices, and more) across industries (transportation, manufacturing, logistics, healthcare, hospitality and more) rises, so do security concerns. Thus, securing company-owned devices and business data from different kinds of threats is paramount for IT teams.

Critical Android Security Vulnerabilities

This is how Google classifies Android security vulnerabilities and ranks them by severity. Let's take a closer look at these vulnerabilities, see how they are commonly exploited, and what kinds of threats they pose to businesses that use Android devices.

1 https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/IDC_Android_Infographic.pdf

Remote code execution (RCE)

Remote Code Execution (RCE) allows attackers to access or make changes to devices they don't own by running a malicious code remotely and without the device owner's knowledge. RCE vulnerabilities are considered to be the most dangerous as it happens through a malicious code run on the vulnerable system or device. For businesses, if exploited, RCE can result in the exfiltration of confidential data, network intrusions, and overall device impairment, harming business functionality.

Generally, RCE-based exploitation happens through email, web browsing and instant messaging apps via media files. RCE can allow an attacker to access the device, extract private data and use it for malicious purposes.

Another way of executing RCE attacks is by exploiting a vulnerability in the way Android devices implement Bluetooth. An attacker can silently execute an arbitrary code (which would run in the background without the user's knowledge) by using Bluetooth privileges.

Key Threat Vectors: *Emails, Web Browsing, MMS media files, Bluetooth, Wi-Fi, and Malicious Apps*

Elevation of Privilege (EoP)

Elevation of Privilege (EoP) is a security flaw that exists in an app or OS and can be exploited by an attacker to gain elevated access. For instance, someone who has only 'read' access to a particular file can gain 'read and write' access using a malicious app. By elevating their privileges, attackers can steal data, run commands by gaining admin access, and damage the OS and/or other apps by deploying malware.

Numerous research articles have shown that EoP can occur through malicious and genuine apps alike. Even Android's security and sandbox model cannot provide protection against malware and runtime attacks.

Sandbox smashing is the most common way to elevate privileges. Attackers seeking additional information may break the application sandbox or root the device. They can do this by exploiting vulnerabilities at the OS, hardware, or application levels. One such vulnerability that made

headlines confirmed that a malicious app exploiting this vulnerability can elevate its access to "root level" temporarily.

Brain Test and HummingBad were similar attacks. Brain Test, bundled in a game in the Google Play Store, was able to bypass Google's security scanning to install a rootkit on the device by exploiting various vulnerabilities of EoP. The malware stayed on the device even after users uninstalled the app. HummingBad was a kind of mobile chain attack targeted to download malicious apps by rooting user' devices.

Key Threat Vectors: *Malicious Apps*

Information Disclosure (ID)

Information Disclosure attacks permit access to hidden or otherwise inaccessible information. At-risk information includes application-specific information (such as underlying frameworks and architecture) or device-level information (such as device MAC addresses or unique identifiers).

Information Disclosure attacks can serve as a gateway to exploiting more threatening vulnerabilities. This can result in the loss of confidential and proprietary information.

One of the most common threat vectors for ID vulnerability is peeking at debug logs. These logs often include developer comments and error messages left due to negligence, allowing hackers to infer a great deal of information about app or system internals. Allowing reads from buffer overflows is another common way in which this vulnerability manifests. Malicious apps can exploit these kinds of vulnerabilities to read protected information.

Key Threat Vectors: *ADB Debugging, System Logs, and Malicious Apps*

Denial of Service (DoS)

In denial-of-service (DoS) attacks, the attackers restrict an authorized user from accessing some on-device data or resources. This kind of vulnerability allows attackers to crash or choke key services on a device. This can occur by flooding the device with requests, or crafting requests to key services that cause the services to crash and thus deny them to all other apps on the device.

These DoS attacks can impair device functionality and performance, disrupting productivity and business continuity.

One such critical vulnerability (discovered and patched by Google) targeted the Media Framework System on Android devices. Attackers could send a specifically crafted message to the device, parsing which Media Framework System could crash and fail to serve other applications on the device. DoS attacks can also target Android devices' Bluetooth capabilities.

Key Threat Vectors: *Bluetooth, MMS, and Malicious Apps*

How can Google (and Device Manufacturers) save us from these vulnerabilities?

Google has been upping its game against the growing list of attackers targeting Android devices. Google is using two main strategies to secure the Android platform.

Security Patches

Google has been releasing monthly security patches via Android Open Source Project (AOSP), fixing vulnerabilities as they are discovered, for the recent 3-4 Android versions. These security patches are generally accompanied by patch releases designed specifically for Google's Nexus and Pixel device models. Device manufacturers then quickly follow up releasing these patches for their respective device models. Google sets strict Compatibility Test Suite (CTS) certifications that mandate device manufacturers to quickly roll out these patches on their device models.

Google is releasing a new Android version almost every year. Now with monthly security patches catering to just the last 3-4 major OS versions, a large number of Android devices are being left vulnerable.

In addition, device manufacturers further limit device support period to just a couple of years, leaving older devices unprotected. Two years of active support with regular security patches is not enough to extract useful ROI, especially for businesses acquiring several thousands of devices at a time.

This situation is made worse by the fact that it's extremely challenging for manufacturers to release security patches on a monthly basis for the huge catalog of device models that they sell. Manufacturers often bundle patches across several months before rolling out over-the-air (OTA) updates. This results in a long gap between vulnerabilities being exposed and devices receiving the patches needed to resolve those vulnerabilities.

Google Play Protect

Google Play Protect has been instrumental in detecting and alerting users about malicious Google Play Store apps installed on devices. Play Protect comes out of the box in Android and is free. Being a part of Play Store and Services, it updates silently behind the scene without requiring OS patch updates. This does offer a mitigation tool for devices where OS update with security patches is not possible.

Despite being free, Google Play Protect has been criticized in the community for its lack of teeth in detecting malwares. Also, it can only offer possible protection against malicious apps. There are a whole lot of other threat vectors like Bluetooth, Wifi, Emails, and more which are mostly unguarded by Play Protect.

How 42Gears' UEM solution helps mitigate Android security vulnerabilities on company-owned devices

Apart from providing device management, 42Gears' UEM solution also offers security policies that protect organizations against the potential exploitation of vulnerabilities on the devices they use. This paper has already established the main threat vectors used for exploiting Android vulnerabilities; let us now take a look at 42Gears' UEM solution that can help us mitigate these vulnerabilities.

Kiosk Mode

The kiosk mode helps manage devices in the field, devices operating as kiosks, and devices intended to be used for particular purposes only. In all these cases, a device needs to be locked down into Kiosk mode.

As corporate-owned devices can contain confidential information, leaving them unattended or uncontrolled makes it easy for attackers to steal data or misuse such devices for malicious purposes (such as downloading malicious apps from the Google Play Store, sending phishing emails, changing Android settings, misusing cameras, and more).

To secure devices against vulnerabilities, 42Gears' UEM solution offers the features below:

- **Allowed apps -** Allow only line-of-business and other essential apps and disable or block access to all other default apps like Phone, Messages, Emails, Camera. Access to any other application on the device is also blocked by Watchdog, killing it automatically the moment it tries to run.
- **Block Play Store -** Revoke access to Google Play Store, preventing users from installing any new unwanted applications.
- **Block access to Android Settings.**
- **Install new apps and updates from the UEM console**, completely moderated by the administrator.
- Define compliance policies to **auto uninstall blocked apps.**

Network Policy

Company-owned Android devices are exposed to different public, unsecured Wi-Fi networks, Bluetooth, and more that make them vulnerable to threats, presenting attackers with an easy way to enter the organizational network. 42Gears' UEM solution allows IT personnel to secure business devices by defining network policies such as:

- **Disable Bluetooth, GPS, Mobile Data** (if not required) - This restricts device users from turning these functionalities on.
- **Allow WiFi SSID** - This allows users to connect to trusted SSIDs only.
- **Firewall policies -** These allow IT admins to:
  - Allow/Block URLs and IP addresses globally on devices and restrict any traffic from such devices to prevent exfiltration.
  - Allow/Block URLs and IP address per app on device.

- **Per app VPN-** This ensures secure and encrypted data transfer.

Security Policy

Android devices can be exploited via SD cards, USB ports and unknown sources. A device, if left unattended, can be misused by attackers by using SD cards, USB Debugging, or installing malicious content from unknown sources. 42Gears uses a security policy to ensure no one can use these techniques to exploit business devices:

- 42Gears' UEM solution can disable SD card, USB debugging, **USB storage, and prevent app installation from unknown sources.**
- 42Gears have Mobile Threat Defence (MTD) scanning, which keeps scanning devices to detect threats and sends alerts to admins for remedial actions.

OS Patch Management

Apart from the above-mentioned capabilities, 42Gears' UEM solution also offers OS patch management features, which include:

- Accurate **reporting of security patch level** across the device fleet.
- **Integration with OEM patch management systems** like Samsung E-Fota, Zebra Lifeguard, and Datalogic firmware update to detect when patches are available and silently push security patches on devices.