LifeGuard™ for Android™
FREQUENTLY ASKED QUESTIONS

ZEBRA

TABLE OF CONTENTS

This FAQ is designed for Zebra partners and end-customers. It is designed to provide end-customers an overview of Zebra's LifeGuard™ for Android™. Please note that Lifeguard™ for Android™ security updates are classified by Zebra as restricted software. As such, they are governed by Zebra's restricted software End User License Agreement (EULA) which means the security software updates can only be downloaded to entitled Zebra devices. Entitled Zebra devices include those devices which are still within the first 90 days (warranty entitlement) or protected by a Zebra OneCareTM Support Services agreement. For additional information, contact your local Zebra representative.

1. WHAT IS LIFEGUARD™ FOR ANDROID™ (LG)?

LG represents an Operating System (OS) security support model for Zebra Android products. LG provides Zebra customers three security value propositions;

1) Extended availability of OS security updates/patches
2) Security support during OS transitions (referred to as an "OS Transition Period")
3) Periodic security patches as frequent as every 30 days.

Life Guard is unique in that it caters specifically to enterprise customers. Extending the security life, extends the device service life, which ultimately reduces TCO (Total Cost of Ownership). Consumer device manufacturers are working diligently to do the exact opposite, i.e. keep support windows short to increase refresh rates and sell more devices.

2. WHY LG NOW?

In 2016 Android & IOS comprised over 99% of the Worldwide mobile OS market share. Though such large-scale adoption brings many benefits, it also creates lucrative targets for hackers. Thus, now more than ever enterprise customers must be more prescriptive and diligent with respect to security maintenance of their mobile operating system. As highlighted in a recent Homeland Security (April 2017) report ("Study on Mobile Security") on enterprise security best practices:

1). "The most important defense against mobile device security threats is to ensure devices are patched against the publicly known security vulnerabilities"

2). "When making procurement decisions, enterprises should seek clear commitment from device vendors or mobile carriers that security updates will be provided in a timely manner"

3). "When a device model is no longer supported with updates, enterprises should decommission those devices"

https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

3. WHAT IS THE POTENTIAL IMPACT OF MOBILE ATTACKS TO ENTERPRISE CUSTOMERS?

It's hard to put an exact dollar amount on mobile attacks, but in general customers should be concerned with; Disruption of Business, Loss of Productivity, Loss of Privacy, Theft of Information, Legal Liability, Brand/Reputation Damage.

It is critical that customers understand the scope of these attacks. A 2016 attack called DressCode enabled a compromised mobile device to be used as a gateway to corporate back-end servers. Thus, even if customers are not storing significant sensitive data on the mobile device, they should still be diligent with security updates.

4. ARE MOBILE VULNERABILITIES ON THE RISE?

Yes, vulnerabilities have risen with increased mobile device functionality, connectivity, and software supply chain contributors. CVE details (www.cvedetails.com) estimates that Android vulnerabilities numbered 611 in 2018.

Recognize that a "vulnerability" is not the same as an "attack." Many headline vulnerabilities (e.g. Stage fright) were never actually detected on any devices outside of a research lab.

5. WHAT ARE OS SECURITY UPDATES?

The terms "Security Updates" & "Security patches" are used synonymously. These are software updates specifically to fortify the underlying Android OS and device specifics from known vulnerabilities.

6. WHAT IS THE DIFFERENCE BETWEEN LIFEGUARD AND MX?

Mx (Mobile extensions) represents Zebra extensions made to standard Android to enhance management and security. These extensions are made available to EMMs, developers (via Zebra EMDK), and Zebra utilities (e.g. StageNow). Some of the Mx features enable disabling or locking down unused device features which "mitigates" or blocks threats.

In contrast, LifeGuard is relegated to security life cycle management and security updates. The updates in LG "remediate" threats. That is, it patches vulnerabilities in the core operating system.

7. UNDER LG, HOW LONG WILL ZEBRA PROVIDE SECURITY UPDATES?

Security updates under LG is based on the device life cycle. Under LG, security patches are made available for the product hardware service life. For Zebra products that is either 6, 8, or 10 years. Note that past OS releases for a given product are generally not supported except as defined under an OS Transition Policy (OTP), which is covered later in this FAQ.

8. CAN END OF SALE DATES SHIFT?

Yes. Zebra typically targets products as available for sale as either 3, 4, or 5 years depending on the type of product. End-of-sale dates may fluctuate based on market conditions and component availability. Zebra works diligently during component selection to align with the planned life cycle, but we cannot make any guarantees.

9. ARE ALL ZEBRA ANDROID PRODUCTS COVERED UNDER LG?

No. Though the vast majority of all recent products are covered under LG, please contact your Zebra representative for the exact level of support for the product of interest.

10. DOES ZEBRA GUARANTEE MY DEVICE IS SECURE IF I AM UP TO DATE?

No. It is often said that security is a journey with no end destination. Security updates are one element in a "defense in depth" security model. That is, a model that provides multiple levels of protection. Customers should install the latest security updates, and leverage standard Android & Zebra Mx features for added protection.

11. WHAT IS A CVE?

CVE's ("Common Vulnerability Exposure") represent security vulnerabilities. All CVE instances have a unique identifier. A database of CVE's can be found at: https://cve.mitre.org/cve/cve.html. Customers can obtain details of a specific CVE through a simple database search.

12. WHAT TYPE OF ATTACKS ARE WE WORKING TO PREVENT?

There are many types of attacks. Some common attacks include; remote code execution, application privilege escalation (permitting application access to resources it should not), disclosure of information on the device, and denial of service attacks. Note that most recent attacks have not been by exploiting OS vulnerabilities, but rather social networking (e.g. phishing).

13. WHAT IS AN ANDROID SECURITY BULLETIN?

Each month (generally early in the month) Google publishes an Android Security Bulletin. Bulletins are labeled by the month in which they were released (January, February…). Google OEM device suppliers (e.g. Zebra) are provided access to the bulletins 30 days prior to the public release. With this notification Google includes patch samples which then must be integrated accordingly into each respective platform. Bulletins include a list of recently discovered Android CVE's along with their respective "severity" level (e.g. Low to Critical).

In 2016 Google addressed a total 655 vulnerabilities (an average of over 50 per month). 133 of these vulnerabilities were ranked as "severe" (~11/month on average). Note that not all CVE's are relevant to all Android products (some are dependent on specific hardware vendors/components).

A description of what constitutes a specific CVE "severity" rating can be found at:
http://source.android.com/security/overview/updates-resources.html#severity

Published Android Security Bulletins can be found at: http://source.android.com/security/bulletin/

14. WHAT IS A PATCH LEVEL?

Applying the updates associated with each bulletin will set the Patch Level as indicated in the Bulletin. This same information is in an individual product's release notes. The Patch Level provides two dates. The first date is your device's most recent full security update. The second date is date your device last received Critical Only updates.

EXAMPLE: Patch Level 2016-05-01 Critical 2016-12-01

The example illustrates that the device was last fully patched in May of 2016 and started receiving critical patches. The last date that Critical patches were applied was December 1, 2016.

You can find the patch level on a device by going into Settings >> About Phone

15. HOW LONG DOES GOOGLE PROVIDE SECURITY SUPPORT FOR ANDROID?

Google typical provides security support for a period of 42 months after an OS release has gone open source.

16. HOW DOES LG OTP HELP CUSTOMERS MAINTAIN SECURITY DURING AN OS TRANSITION?

Under LG, when Zebra releases a new OS version (desert release) for a product, we continue to support the earlier version for a period of 12 months. This is referred to as an OS Transition Period (OTP). During OTP, customers receive quarterly (exact cadence may fluctuate slightly) updates with a minimum coverage for all "critical" severity CVE's.

17. DOES LG SUPPORT CHANGE DURING PRODUCT/OS LIFE CYCLE (L1, L2, L3)?

LG has three support levels; L1, L2, L3. Except where explicitly stated, the scope of all support levels is the Google Android Security bulletins. L1 is the highest level of support and is provided for the latest OS release for a product during the period in which Google is providing security support. L2 has slightly less support and is provided for an older OS during an OS Transition Period, and for the latest OS during the period after Google stops security support and prior to Zebra end of support (EoS + 2 yrs).

L1 - during L1 Zebra provides updates approximately every 30 days. Updates are comprehensive, in that all relevant Android Security Bulletin CVE's regardless of severity level are addressed. L1 support is provided for the latest current OS release on a product during the period in which Google is providing security support updates.

L2 - during L2 Zebra provides quarterly updates minimally covering all Android Security Bulletin CVE's posted as "critical." L2 support is provided during two periods. The first is during an OS Transition Period (OTP). The second is the period after Google has terminated security support and prior to Zebra's end of security support.

L3 - Products not in either L1 or L2 fall into a Zebra discretionary support window (L3), during which Zebra will make a best effort to address major security vulnerabilities.

18. HOW MUCH DOES LG COST?

LG is zero cost for customers covered under any of the following Zebra agreements;

1) Zebra Initial Purchase Software Warranty
2) Zebra OneCare Essential
3) Zebra OneCare Select
4) Zebra OneCare TSS (Technical and software support – excludes break-fix repair)

One-year OS security support extensions are available at additional cost.

Descriptions of the OneCare options can be found at:
https://www.zebra.com/us/en/services/run/support-services/zebra-onecare/onecare-enterprise.html

19. CAN I ADD SUPPORT TO A PRE-EXISTING PORTFOLIO NOT ALREADY COVERED UNDER A SERVICE PLAN?

Yes, you can purchase a OneCare service contract inclusive of LG. However, there may be an added service charge depending on the specific device/OS platform(s) that you are looking to cover. Please contact your local Zebra representative for additional information.

20. CAN I EXTEND LG SUPPORT? HOW MUCH DOES IT COST? HOW DO I PROCURE?

Yes but within limits. You can extend the OS Transition Period for up to 1 year. Extending an OTP allows the customers added time (i.e. another 12 months) to transition between OS releases while still getting security updates. The scope of the one-year extension is to a specific product model on a specific OS release (identified within the purchase agreement).

Support during the extension period is L2 (Quarterly updates /Critical severity). The agreement only covers security support and does not entitle the customer to general bug fixes or maintenance releases. In some instances, a security patch may be contingent on a bug fix/MR, in which case Zebra will make the necessary bug fix/MR available to the customer. In many instances these security updates may fall outside of the Google Support window. Though an exception condition, certain security vulnerabilities may be systemic; requiring significant changes that would impact the stability and interoperability of the platform of an earlier OS release. In such cases, Zebra cannot guarantee that it will directly re-mediate every such vulnerability. Therefore, Zebra will provide remediation recommendations, but may not provide a code patch/update for such vulnerabilities.

Under the one-year extension agreement, Zebra will provide limited phone support. Often referred to as “Level 1” escalation this will be relegated to basic question & answers.

Contact your Zebra representative for pricing information.

21. CAN I PURCHASE A ONE (1) YEAR EXTENSION AT ANY TIME?

No. A customer can only purchase an extension if the product/OS is under existing security support. The extension must be purchased no less than 90 days prior to the end of the customer’s existing support contract. There is no set price for this feature, please contact a Zebra representative for additional information.”

22. WHAT DO CONSUMER COMPANIES OFFER FOR SECURITY UPDATES?

Many consumer device providers do not offer a formal security update policy. Google does for their Nexus & Pixel devices. Nexus & Pixel are generally considered the gold standard for consumer grade support. Google provides security support for the later of either 36 months from first ship or 18 months past end-of-sale. In general consumer device life cycles are less than 18 months, so typical support is relegated to the 36 months from first ship. In comparison, a Zebra 5/5 product offers 120 months of support.
https://support.google.com/pixelphone/answer/4457705?hl=en

23. WHERE DO I FIND SECURITY UPDATES?

Security updates can be found at: https://www.zebra.com/us/en/support-downloads/lifeguard-security.html.

24. HOW ARE SECURITY PATCHES INSTALLED ON A DEVICE? LOCAL? EMM OTA?

Security patches can generally be installed either over USB via ADB, using an external SD card (if supported), or over-the-air (OTA) via an EMM (consult Zebra for validated EMMs).

25. HOW LARGE ARE TYPICAL SECURITY UPDATES?

Sizes can vary significantly. Security updates bundled with bug fixes and maintenance releases will be larger in size. Typical updates will be 40-50MB.

26. CAN I REVERSE/ROLLBACK A PATCH?

Yes. In the atypical situation where you have to reverse a patch, you can do so by either installing an earlier patch level or issuing a factory reset.

27. HOW DO I TELL WHAT SECURITY UPDATES HAVE BEEN LOADED ON MY DEVICE?

The Patch Level provides the date the last monthly and quarterly critical only updates.

28. ARE SECURITY UPDATES ALWAYS SEPARATE FROM OTHER MAINTENANCE RELEASES?

No. Security updates may be either separate or bundled with bug fixes and maintenance releases

29. ARE SECURITY UPDATES CUMULATIVE?

Yes. If you opted to forego loading some earlier update, loading a newer update will load the previous and current updates.

30. DO SECURITY UPDATES COME WITH RELEASE NOTES?

Yes. Release notes are posted with the security update.

31. CAN I BE NOTIFIED WHEN A PATCH IS AVAILABLE FOR MY PLATFORM?

Yes. You can subscribe for email notifications at:
https://www.zebra.com/us/en/forms/request-lifeguard-updates.html

32. DO I HAVE TO BE ON THE LATEST MAINTENANCE RELASE TO INSTALL AN UPDATE***?

Yes. Zebra cannot validate security on all incremental maintenance releases, therefore, you must be on the latest maintenance release prior to loading the security update.

33. HOW LONG WILL IT TAKE ZEBRA TO RELEASE A SECURITY UPDATE AFTER A SECURITY BULLETIN?

Zebra's goal is to be within 2-3 days of the public Android security bulletin. However, many updates vary in complexity and scope, and have dependencies on third party code that must be obtained by Zebra. Thus, security updates may vary depending on the region, product model, and third-party software suppliers. Additionally, releases for WAN (cellular) devices may lag other release due to additional testing and/or carrier certification. Carrier certifications can vary from 2 wks to 6 wks depending on the specific carrier and the extent of required testing.

Note also that an update may be a combination of a maintenance release and a security update.

Finally, because of the lag time in carrier certification it is possible that a carrier certified update may actually have a security patch level earlier than a prior release. Thus, when loading a new, major, carrier certified update, customers should check the patch level and if necessary load the necessary patches.

34. DOES ZEBRA ADVISE CUSTOMERS TO INSTALL ALL UPDATES?

Zebra does advise customers to install all updates in a timely manner. However, we appreciate that all software updates carry some degree of functional risk. Customers operating in a peak season (and a potential code lockdown) may want to assess the individual CVE's being addressed in a release. Customers may already be using techniques that mitigate many these CVEs (e.g. application white listing, enterprise home screen, lock task mode). Though updates will provide an added level of defense (defense in depth) customers should make an informed decision.

35. ARE ZEBRA UPDATES EVER COVERTLY PUSHED TO DEVICES?

No. In contrast to other platforms (e.g. IOS), Zebra does not push updates either overtly (e.g. user receives a message asking to accept update) or covertly directly to devices.

36. DOES ZEBRA PROVIDE SECURITY PATCHES FOR GMS?

No. Zebra devices are either AOSP or GMS. Technically Google Mobile Services (GMS) sits above AOSP. In contrast to AOSP which is open source, GMS is closed binary, owned by Google. GMS updates (including security enhancements) are provided by Google.

GMS updates come from the Google Play Store and typically requires a Google account (Managed Account or Google Account) be present on the device (note: Google has the right to push an update without an account).

37. WHAT ABOUT ZERO-DAY ATTACKS?

Occasionally a major attack instantly surfaces. These attacks cannot be predicted and it is difficult to predict a response time. Zebra does however monitor for such attacks and has responded in real time in the past.

38. AFTER GOOGLE ENDS SUPPORT, HOW DOES ZEBRA DETERMINE WHAT TO PUSH?

The principal source for Zebra updates are the Android security bulletins. This is true both during Google support for an OS release and after Google ends support. Thus, post Google support, Zebra assess each vulnerability and determines how to backport relevant patches (if possible).

Note that during this period, certain security vulnerabilities may be systemic; requiring significant changes that would impact the stability and interoperability of the platform of an earlier OS release. In such cases, Zebra cannot guarantee that it will directly remediate every such vulnerability. Therefore, Zebra will provide remediation recommendations, but may not provide a code patch/update for such vulnerabilities.

39. AFTER GOOGLE ENDS SUPPORT FOR AN OS RELEASE, DOES ZEBRA GUARANTEE THAT ALL VULNERABILITIES ARE PATCHED?

We do our best, but we cannot guarantee that all vulnerabilities will be patched. After Google has ended security support for an OS release (e.g. a desert OS), Zebra continues to monitor the newer Google monthly updates. We analyze each vulnerability in the update to determine if it is applicable to the older (unsupported by Google) OS release. If it is, we take the patch and "backport" (the process of taking a newer patch and adapting it to an older OS). We can only backport updates in cases where the functionality previously existed and/or the update does not impact the integrity of the platform.

40. DO I NEED LIFEGUARD FOR PCI COMPLIANCE?

Zebra is not a PCI Qualified Security Assessor (QSA), with whom we suggest you consult. PCI DSS 3.2 does not appear to have this as a hard dependency. However, PCI DSS 3.2 Section 6.4.5 (Change control procedures) Guidelines, states; "if not properly managed, the impact of system changes – such as hardware or software updates and installation of security patches – might not be full realized and could have unintended consequences."

41. WHAT IS THE LIFECYCLE FOR GMS UPDATES?

As stated earlier, Google owns and maintains GMS. Though Google has no public policy, in Nov 2016 Google announced that the latest GMS would not support GB 2.3.7. This equates to a period of over 5 years. Obsoleted devices will continue to operate but will not receive any updates (including security updates).

42. WHAT IS THE LIFECYCLE FOR EMM UPDATES?

Zebra does not control EMM life cycle. Our experience has been that EMM's support legacy Operating Systems for ~5-6 years. Console operation will generally continue beyond this window, but new features and security support will no longer be available. Consult your EMM for any updates.

43. DOES LIFEGUARD PROVIDE SECURITY UPDATES FOR GMS?

Zebra Android "GMS devices" actually consist of two major software components; Android Open Source Project (AOSP) and Google Mobile Services (GMS). AOSP is open source while GMS libraries are closed binaries licensed and provided by Google. The GMS libraries are typically updated by Google from the Android Play Store (access to the play store is required). The only exception will be when Zebra provides a complete image update, in which case the GMS libraries will be provided as part of that update. Note that the GMS version in the Zebra provided update may not be the latest. Customers with applications leveraging GMS services should enable a connection to the Play Store enabling a GMS update.

44. CAN CUSTOMERS STILL OBTAIN A LOCKED DOWN IMAGE VIA A CUSTOM PRODUCT REQUEST?

Yes, however we have had customers inquiring about a semi-locked image that would include security updates with no maintenance updates. This is still under consideration.

45. WHAT IF A CUSTOMER DETECTS A VULNERABILITY?

Customers that detect a vulnerability can securely report that vulnerability by going to:
https://www.zebra.com/us/en/forms/lifeguard-vulnerability.html

46. WHAT IS THE ZEBRA URL TO ACCESS THE LIFEGUARD SECURITY UPDATES?

https://www.zebra.com/us/en/support-downloads/lifeguard-security.html