kony™

Kony Security Brief:

Addressing the OWASP Mobile Top 10 with Kony MobileFabric™ and Frameworks

Kony addresses mobile threats through our Mobile Application Development Platform and frameworks, as well as our Mobile Backend as a Service (MBaaS). This document provides a summary of how these vulnerabilities are addressed by Kony.

MobileFabric

Weak Server Side Controls (M1)

The OWASP Top 10 vulnerabilities (and more) are addressed through secure configuration and coding practices in our software development lifecycle (SDLC) that directly benefit Kony web services and APIs. In addition, Kony addresses the OWASP Application Top 10 and beyond for our web applications and web services.

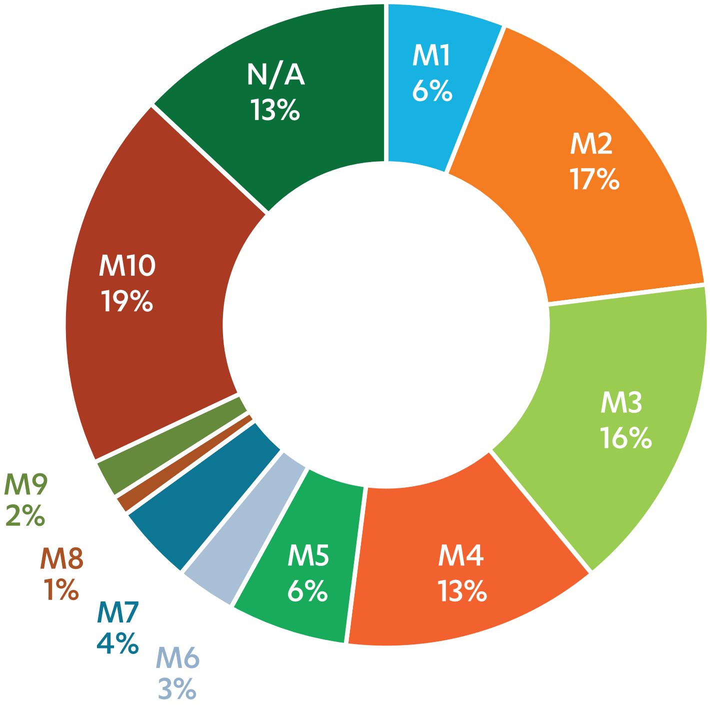
Insufficient Transport Layer Protection (M3)

Addressed through secure configuration of the server and coding of the mobile application. Strong industry standard cipher strengths and key lengths are used, while vulnerable protocols are disabled. In addition, Kony provides the ability to use certificate pinning and mutual authentication (2-way SSL) to prevent man-in-the-middle (MITM) attacks. In addition, Kony's data encryption APIs supports both symmetric and asymmetric encryption. These can be used as an added layer of protection. In a scenario where another serious vulnerability is discovered in the SSL protocol that might allow information disclosure, the data would still be protected with its own encryption.

Poor Authorization and Authentication (M5)

Kony's MobileFabric Identity Server manages authentication and authorization. JSON Web Token (JWT) is used between the mobile application and MobileFabric. In addition, MobileFabric authentication supports OAuth2, SiteMinder, Active Directory, and more. Authorization validation is performed for each business transaction while authentication controls are provided to meet the requirements of Kony's customers.

OWASP Mobile: Top 10 Vulnerabilities



Improper Session Handling (M9)

MobileFabric utilizes JSON Web Token (JWT) protocol for authentication, an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with HMAC algorithm) or a public/private key pair using RSA. Tokens are securely created and transmitted over secure channels using industry standards. By leveraging claims by including a nonce (jti claim), expiration time (exp claim), and creation time (iat claim) we prevent replay attacks. These are well defined in the JWT Spec.

Frameworks

Insecure Data Storage (M2)

Kony provides secure methods for storing and transmitting data, including whitebox cryptography as an additional layer of encryption beyond any default encryption mechanisms provided by the operating system. Furthermore, Kony provides out-of-the-box encryption to protect source code and other resources.

Unintended Data Leakage (M4)

Kony provides APIs to address unintended data leakage by providing the means to prevent: screen captures, application backgrounding, application data backups, copy/pasting, keyboard press caching, URL caching, logging, HTML5 data storage, browser cookie objects, 3rd party analytic data, etc.

Broken Cryptography (M6)

Kony provides powerful secure cryptography capability beyond the native operating system's capabilities. Kony encryption and decryption uses a secure process known as whitebox cryptography to perform encryption and decryption while keeping keys safe. Strong algorithms are used for encryption and decryption; insecure and deprecated algorithms are not used.

Client Side Injection (M7)

A combination of security mechanisms prevent client side injection attacks via communication channels between the client and server, in addition to preventing injection attacks via binary injection and modification. A variety of API options are provided to disable WebViews to prevent cross-site scripting, parameterized queries to prevent SQL injection, parsing libraries that are resilient to parsing attacks, and the ability to properly perform input validation in the client application to prevent a wide array of input validation based attacks.

Security Decisions Via Untrusted Inputs (M8)

Input validation is performed on both the client and server side. If Inter Process Communication (IPC) calls must be used then they are required to undergo stringent input validation, require user interaction for sensitive actions, and are whitelisted to the applications necessary.

Lack of Binary Protections (M10)

Binary protections slow down and can prevent an adversary from:

- Analyzing exposed interfaces and reverse engineering code within the mobile app
- Modifying the underlying code or behavior to disable or add additional functionality

Static Protection

- Code obfuscation
- Control flow obfuscation
- Call hiding
- Symbol stripping
- Anti-tampering

Dynamic

- Code obfuscation
- Code injection prevention
- Hook prevention
- Debugger prevention
- Root & jailbreak detection

Kony is the fastest-growing, cloud-based enterprise mobility solutions company and an industry leader among mobile application development platform (MADP) providers. Kony empowers today's leading organizations to compete in mobile time by rapidly delivering multi-edge mobile apps across the broadest array of devices and systems, today and in the future. Kony offers ready-to-run business mobile apps to help organizations better engage with customers and partners, as well as increase employee productivity through mobile device access to company systems and information. Powered by Kony's industry-leading Mobility Platform, enterprises can design, build, configure, and manage mobile apps across the entire software development lifecycle, and get to market faster with a lower total cost of ownership.

For three years in a row, Gartner has named Kony a Leader in its Magic Quadrant for Mobile Application Development Platforms. In addition, Kony was named a "Leader" and earned the highest score in the current offering category in Mobile Infrastructure Services by independent research firm Forrester Research, Inc., according to The Forrester Wave™: Mobile Infrastructure Services, Q3 2015 report. In additional to these recognitions, Kony was also honored in the Mobile Star Awards for achievements in enterprise application development; named the first place winner in CTIA's MobITs Awards in the Mobile Applications, Development & Platforms category, and included on the Inc. 500|5000 list of fastest growing private companies in America.

For more information, please visit www.kony.com. Connect with Kony on Twitter, Facebook, and LinkedIn.
9225 Bee Cave Road, Building A, Suite 300, Austin, TX 78733 1.888.323.9630 | info@kony.com | kony.com