Application Developer Guidance, Mitigation M1013 - Mobile

Archived: 2026-04-05 15:47:53 UTC

Enterprise T1212 Exploitation for Credential Access

Application developers should consider taking measures to validate authentication requests by enabling one-time passwords, providing timestamps or sequence numbers for messages sent, using digital signatures, and/or using random session keys.[1][2]

Enterprise T1564 Hide Artifacts

Application developers should consider limiting the requirements for custom or otherwise difficult to manage file/folder exclusions. Where possible, install applications to trusted system folder paths that are already protected by restricted file and directory permissions.

.009 Resource Forking

Configure applications to use the application bundle structure which leverages the `/Resources` folder location.[3]

.012 File/Path Exclusions

Application developers should consider limiting the requirements for custom or otherwise difficult to manage file/folder exclusions. Where possible, install applications to trusted system folder paths that are already protected by restricted file and directory permissions.

Enterprise T1574 Hijack Execution Flow

When possible, include hash values in manifest files to help prevent side-loading of malicious libraries.[4]

.001 DLL

When possible, include hash values in manifest files to help prevent side-loading of malicious libraries.

Enterprise T1559 Inter-Process Communication

Enable the Hardened Runtime capability when developing applications. Do not include the `com.apple.security.get-task-allow` entitlement with the value set to any variation of true.

.003 XPC Services

Enable the Hardened Runtime capability when developing applications. Do not include the `com.apple.security.get-task-allow` entitlement with the value set to any variation of true.

Enterprise T1647 Plist File Modification

Ensure applications are using Apple's developer guidance which enables hardened runtime.[5]

Enterprise T1496 .003 Resource Hijacking: SMS Pumping

Consider implementing CAPTCHA protection on forms that send messages via SMS.

Enterprise T1593 Search Open Websites/Domains

Application developers uploading to public code repositories should be careful to avoid publishing sensitive information such as credentials and API keys.

.003 Code Repositories

Application developers uploading to public code repositories should be careful to avoid publishing sensitive information such as credentials and API keys.

Enterprise T1195 Supply Chain Compromise

Application developers should be cautious when selecting third-party libraries to integrate into their application. Additionally, where possible, developers should lock software dependencies to specific versions rather than pulling the latest version on build.[6]

.001 Compromise Software Dependencies and Development Tools

Application developers should be cautious when selecting third-party libraries to integrate into their application. Additionally, where possible, developers should lock software dependencies to specific versions rather than pulling the latest version on build.[6] GitHub Actions may be pinned to a specific commit hash rather than a tag or branch.[7]

Enterprise T1550 Use Alternate Authentication Material

Consider implementing token binding strategies, such as Azure AD token protection or OAuth Proof of Possession, that cryptographically bind a token to a secret. This may prevent the token from being used without knowledge of the secret or possession of the device the token is tied to.[8][9]

.001 Application Access Token

Consider implementing token binding strategies, such as Azure AD token protection or OAuth Proof of Possession, that cryptographically bind a token to a secret. This may prevent the token from being used without knowledge of the secret or possession of the device the token is tied to.[8][9]

Enterprise T1078 Valid Accounts

Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).

Mobile T1626 Abuse Elevation Control Mechanism

Applications very rarely require administrator permission. Developers should be cautioned against using this higher degree of access to avoid being flagged as a potentially malicious application.

Mobile T1517 Access Notifications

Application developers could be encouraged to avoid placing sensitive data in notification text.

Mobile T1513 Screen Capture

Application developers can apply the `FLAG_SECURE` property to sensitive screens within their apps to make it more difficult for the screen contents to be captured.[10]

Mobile T1635 Steal Application Access Token

Developers should use Android App Links[11] and iOS Universal Links[12] to provide a secure binding between URIs and applications, preventing malicious applications from intercepting redirections. Additionally, for OAuth use cases, PKCE[13] should be used to prevent use of stolen authorization codes.

.001 URI Hijacking

Developers should use Android App Links[11] and iOS Universal Links[12] to provide a secure binding between URIs and applications, preventing malicious applications from intercepting redirections. Additionally, for OAuth use cases, PKCE[13] should be used to prevent use of stolen authorization codes.

Mobile T1474 Supply Chain Compromise

Application developers should be cautious when selecting third-party libraries to integrate into their application.

.001 Compromise Software Dependencies and Development Tools

Application developers should be cautious when selecting third-party libraries to integrate into their application.
