FirstNet Application Testing and Security Requirements

FirstNet Security Requirement

Preproduction static analysis security scanning for FirstNet mobile apps as well as for new and updated releases of these mobile apps is required. Critical/high vulnerabilities must be remediated prior to submission and production deployment of mobile apps.

FirstNet Listed:

Developers do **not** have to submit a security scan report. FirstNet app review team will scan the binary as part of security evaluation at no cost to the developer.

If the app does not pass the FirstNet security evaluation, the app review team shall provide the developer information on the areas that did not pass. The developer should review the information, fix any identified issues, and resubmit app in App Control.

FirstNet Certified:

Developers must utilize Checkmarx Cx Suite™ or Fortify Static Code Analyzer™ to analyze the app source code.

The developer should review the results of the report and fix any identified issues, prior to app submission in App Control. If fixes are made, a new source code scan must be complete. **The final source code scan result must be provided as part of the app submission.** If fixes are made, a new source code scan must be complete. **The final source code scan result must be provided as part of the app submission.**

The developer should note any false-positives in the scan report. Reasons for false-positives need to be documented within the tool and displayed in the report for auditing purposes.

The developer should ensure the name of the app and the version number are within the source code scan report, and in the filename of the report.

Scanning Requirements

The security analysis scan process must look for vulnerabilities in these areas, but not limited to:

1. Identification and Authentication:
    - replay attacks • authentication by-pass
2. Authorization:
    - backdoors

Last Modified: February 21, 2018

- escalation of privilege attacks
- authorization by-pass

3. Access controls
   - No unauthorized access to data from other mobile apps or users
   - By-pass of access controls
   - Weak or non-existent access controls
4. Injection attacks
   - SQL, Cross-site scripting, buffer overflow, cross-site request forgery
5. Input validation
   - input must be validated for type, size, and value
6. Denial of service attacks
7. Compliance: PCI, HIPAA, CPNI
8. Malware
   - spyware, viruses, botnets, trojan horses, time bombs, worms
9. Secure storage of sensitive data
10. Secure transmission of sensitive data
11. Industry standard encryption techniques are used
12. Secure session management
13. Information leakage
    - No secrets in log files, configuration files, or source code comments
    - No leakage of data to 3rd party sites
    - No leakage of data in error messages
    - No stack traces shown to users
14. Bad code:
    - dead code
    - unhandled exceptions
    - static strings with sensitive data
    - vulnerable or unpatched libraries or frameworks
    - development code used only for testing

Reporting Requirements

Vulnerabilities identified by the scan will be classified as informational, low, medium, or high/critical impact. Scan requires that high vulnerabilities be remediated and validated prior to security review and production deployment of mobile apps. Medium and low vulnerabilities must be analyzed and informational vulnerabilities should be analyzed as they may be a security concern; remediation plan with date and/or reasons for not exploitable must be documented within the scanning tool next to each vulnerability, which will then appear in the final report.

Final report must be provided when submitting a mobile app submission as evidence of the security scan. Neglecting to provide an 'analyzed' report will result in delay of the security review.

Note: FirstNet security analyst will fail an assessment if the above reporting requirements are not followed, i.e. unanalyzed scan reports, in which we will ask the developer to resubmit a new assessment once the report is analyzed with proper remediation plan/fix dates and reasons for 'not exploitable' or 'not an issue' items within the report. All remediation plan/fix dates/reasons must be contained within the report to avoid searching through emails or other files and is required for Audit.

Submitting Scan Results with Submission

In order to be listed in the FirstNet App Catalog, the application will need to undergo rigorous security testing. Apps will be analyzed both statically and dynamically for security vulnerabilities. Such tools and assessments will be continually used, even after an application has been certified, because the security landscape changes with new risks and vulnerabilities discovered daily.

FirstNet is committed to providing the public safety community with secure apps. In order to do so, developers must provide both the security scan and video optimizer scan results as part of their app submission in App Control, with the accompanying Developer Checklist.

Recommended Tools

Choose an approved tool that will perform static code analysis on mobile applications. Mobile source code includes JavaScript, HTML5, Cascading Style Sheets, ActiveX, Flash, as well as native code like Objective-C and Java. Source code scanning is performed on the 'uncompiled' source code files. The Checkmarx Cx Suite and Fortify Static Code Analyzer tools are currently the only tools documented that meet FirstNet requirements for FirstNet Certified source code security scanning. Approved source code or binary scans are acceptable for meeting FirstNet Listed requirements.

Static Analysis Tool	FirstNet Certified	Vendor Information
Checkmarx Cx Suite	✓	Checkmarx Cx Suite (www.checkmarx.com): Scans HTML5, JavaScript, CSS, and any other code that executes in the mobile web context to look for vulnerabilities. Checkmarx's Cx Suite scans source code without requiring the code to be buildable. Cx Suite is very suitable for scanning scripted code as well as native code, 3rd party libraries, and code fragments.

Fortify Static Code Analyzer*	✓	Micro Focus Fortify Static Code Analyzer (https://software.microfocus.com/enus/products/static-code- analysissast/overview): Scans source code and searches through vulnerabilities in every possible path of execution through the code.

*Note: Former software division of Hewlett Packard Enterprise is now part of Micro Focus

Cross Listed Apps

Apps hosted in third party stores and cross-listed in the FirstNet App Catalog, will be audited to ensure version alignment and security.

If any version differences or vulnerabilities are found, FirstNet will notify the developer of the version mismatch and the app will be disabled from further distribution in the FirstNet App Catalog until the developer has submitted a new version and/or remediation plans/commitment date of fix.

Version Updates and Found Vulnerabilities

In instances of undocumented version updates or vulnerabilities found in published products:

- The developer must submit a new app version and/or remediation plans/commitment date of fix within **5 business days** from notice.
- If the developer does not take action after **8 business days** from notice, all apps under review for the developer will be halted.
- If the developer does not take action after **33 business days** from notice, the developer and all of their apps will be removed.

Developers must provide both the security scan and video optimizer scan results as part of their app submission in App Control, with the accompanying Developer Checklist for all code based changes to the app.