'FirstNet Certified' Requirements for Static Analysis Security Scanning

Security Requirement: Preproduction static analysis security scanning for FirstNet Certified mobile apps as well as for new and updated releases of these mobile apps. Critical/high vulnerabilities must be remediated prior to submission and production deployment of mobile apps. Developer is required to purchase an approved tool. Tools can be integrated using a SaaS solution or integrated into the developers IDE.

- **FirstNet Certified:** Developers must utilize Checkmarx Cx Suite^{TM} or Fortify Static Code Analyzer^{TM} to analyze the app source code. See table at the end of this document.

Source code scanning requirements: The source code scan process must look for vulnerabilities in these areas:

1. Identification and Authentication
   - replay attacks
   - authentication by-pass
2. Authorization:
   - backdoors
   - 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 low, medium, or high/critical impact. The developer who is familiar with the code must analyze the report. First, classify all vulnerabilities as either "confirmed" or "not exploitable/not an issue", *then* develop a remediation plan and fix date for any confirmed vulnerabilities. Note that all critical/high vulnerabilities classified as confirmed must be remediated prior to security review and production deployment of the mobile application. For the medium/low "confirmed" vulnerabilities, document the remediation plan and fix date next to each vulnerability within the scanning tool. For vulnerabilities determined "not exploitable/not an issue", explain why they are not exploitable/not an issue next to each vulnerability within the scanning tool. Informational vulnerabilities should be analyzed as they may be a security concern. A source code security scan report must be presented to the FirstNet Security Analyst that displays all developer documentation in the report for auditing purposes.

The developer must include in the system generated report, provided in .pdf format:

- Name of the app and version number within the source code scan report
- Name of app and version number as part of the filename of the report
- Time & date the scan was run
- Version of the scanner used
- Number of or List of files scanned (static file listing) and/or Line of Code count
- Scan policy that was used
- Report must include ALL findings (no exclusions)
- Code snippets
- Annotations next to each vulnerability as indicated in above 'Reporting Requirements'

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 app owner 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 Report 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 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.

Static Analysis Tool	FirstNet Certified	Approved Type of Scan	Vendor Information
Checkmarx Cx Suite	✓	Source code scan	Checkmarx Cx Suite (www.checkmarx.com)
Fortify Static Code Analyzer	✓	Source code scan	Micro Focus Fortify Static Code Analyzer (https://software.microfocus.com/en-us/products/static-code-analysis-sast/overview)

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.