Injet New Energy Vulnerability Management Guidelines

1. Introduction

1.1 Purpose

This document is intended to define the vulnerability management process for Injet New Energy's electric vehicle chargers products, ensuring the security of all systems, applications, and network components. Through systematic vulnerability management, we can promptly discover, assess, remediate, and track security vulnerabilities, thereby reducing potential security risks.

1.2 Scope

This vulnerability management document applies to all internal and external chargers systems, applications, network services, and related third-party services of Injet New Energy.

1.3 Roles and Responsibilities

- **Security Team:** Responsible for the discovery, assessment, response, and tracking of vulnerabilities.
- **Development Team:** Responsible for the remediation of vulnerabilities.
- **Testing Team:** Responsible for the validation and deployment after vulnerability remediation.
- **Compliance and Audit Team:** Responsible for overseeing the execution of the vulnerability management process and ensuring compliance with relevant regulations and standards.

2. Vulnerability Management Process

2.1 Vulnerability Discovery

- **Automated Scanning:** Regular scanning using the OpenVAS tool.
- **Internal Audits:** Discovering vulnerabilities through code reviews and penetration testing.
- **Third-Party Reports:** Receiving security reports from third parties.

2.2 Vulnerability Assessment

- **Scoring:** Using the CVSS (Common Vulnerability Scoring System) scoring system to rate vulnerabilities.
- **Classification:**
    - **Critical Vulnerabilities:** CVSS score of 9.0 or higher; immediate response required.
    - **High Vulnerabilities:** CVSS score of 7.0-8.9; prompt response required.
    - **Medium Vulnerabilities:** CVSS score of 4.0-6.9; response according to schedule.
    - **Informational Vulnerabilities:** CVSS score of 0-3.9; response based on specific circumstances.

2.3 Vulnerability Response

- **Response Timeline:**
    - **Critical Vulnerabilities:** Respond and begin remediation within 24 hours.
    - **High Vulnerabilities:** Respond and begin remediation within 7 days.
    - **Medium Vulnerabilities:** Respond and begin remediation within 30 days.
    - **Informational Vulnerabilities:** Response time determined based on specific circumstances.

- **Response Actions:**
    - **Temporary Mitigation Measures:** Implement temporary measures to mitigate risk before permanent fixes are applied.
    - **Notification:** Notify affected departments and users, providing necessary guidance.

2.4 Vulnerability Remediation

- **Remediation Workflow:**
    - **Development Team:** Write fix code or configuration changes.
    - **Code Review:** Fix code must undergo code review to ensure no new vulnerabilities are introduced.
    - **Testing Team:** Conduct unit tests and integrity tests post-fix to ensure functionality remains intact.
- **Verification and Closure:**
    - **Verification:** Verified by the Testing and Security Teams to confirm the vulnerability has been fixed.
    - **Closure:** Close the vulnerability record in the vulnerability management system.

2.5 Continuous Monitoring

- **Monitoring Tools:** Use the OpenVAS tool for continuous system monitoring to prevent new vulnerabilities.
- **Regular Reviews:** Conduct quarterly vulnerability reviews to ensure previously fixed vulnerabilities do not reappear.

3. Tools and Technologies

- **Vulnerability Scanning Tool:** OpenVAS
- **Static Code Analysis Tool:** cppcheck
- **Log Analysis Tool:** easylogger

4. Vulnerability Reporting and Documentation

4.1 Report Format

- **Title:** Vulnerability Name
- **Description:** Detailed description of the vulnerability.
- **Severity:** High, Medium, Low, Informational
- **Impact Scope:** Affected systems and components.
- **Recommended Actions:** Suggested fixes.
- **Discovery Date:** Date the vulnerability was discovered.
- **Fix Date:** Date the vulnerability was fixed.
- **Status:** Unfixed, In Progress, Fixed

4.2 Documentation System

- **Vulnerability Management System:** iMIS-PM
- **Documentation Content:** Vulnerability details, remediation progress, verification results, etc.

4.3 Notification Mechanisms

- **Email Notifications:** Sent via the company email system.
- **Instant Messaging:** Use Microsoft Teams for instant notifications.
- **Meetings:** Hold emergency meetings as necessary.

5. Appendix

5.1 Glossary

- **CVSS:** Common Vulnerability Scoring System
- **SIT:** Security Incident Team
- **iMIS-PM:** A project management and issue tracking tool

5.2 References

- **NIST SP 800-53:** Security Controls Guide published by the National Institute of Standards and Technology (NIST)
- **ISO/IEC 27001:** International Information Security Management Standard

5.3 Contact Information

- **Head of Security Team:** Zhang Qin
- **Phone:** +86 18628961761
- **Email:** evse.support@injet.com