Vulnerability Disclosure Report – Fragebogen

Kontaktinformationen

Name / Pseudonym *: _____
(Kann auch ein Handle/Nickname sein)

E-Mail-Adresse *: _____
(Für die Kommunikation während des Prozesses)

Alternative Kontaktmöglichkeit: _____
(z.B. Signal, Telegram, PGP-Key)

Organisation/Zugehörigkeit: _____
(Falls Sie für eine Organisation/Firma forschen)

Möchten Sie in unserer Hall of Fame genannt werden?
☐ Ja, mit Name/Handle: _____
☐ Nein, anonym bleiben

[* - Pflichtfeld]

Betroffenes Produkt

Produktkategorie: (Bitte auswählen)

☐ Smartphone
☐ Tablet
☐ IoT-Gerät (Windows 11 IoT)
☐ Firmware/System-Software
☐ Mobile App
☐ Web-Service/Backend
☐ Sonstiges: _____

Produktname/Modellbezeichnung: _____
(z.B. "ModelX Pro", "TabletY 2024")

Firmware-/Software-Version _____:
(z.B. "Android 14.0.1 Build 20240115", "Windows 11 IoT LTSC 2024 v10.0.26100.2161")

Hardware-Revision (falls relevant): _____
(z.B. "Rev 2.1", "Hardware-ID: XYZ123")

Schwachstellendetails

Titel der Schwachstelle (max. 100 Zeichen)

_____
_____
_____
_____
_____

Schwachstellentyp: (Mehrfachauswahl möglich)
☐ Remote Code Execution (RCE)
☐ Privilege Escalation
☐ Authentication Bypass
☐ SQL Injection
☐ Cross-Site Scripting (XSS)
☐ Buffer Overflow
☐ Information Disclosure
☐ Denial of Service (DoS)
☐ Cryptographic Weakness
☐ Hardware-Schwachstelle
☐ Firmware-Schwachstelle
☐ Treiber-Schwachstelle
☐ Sonstiges: _____

Betroffene Komponente:
☐ AOSP/Android-System
☐ Eigene Firmware-Modifikationen
☐ Hardware/Bootloader
☐ Windows IoT System
☐ Eigene Treiber
☐ Kernel
☐ System-App/Service
☐ User-App
☐ Netzwerk-Stack
☐ Sonstiges: _____

Detaillierte Beschreibung:
Bitte beschreiben Sie die Schwachstelle ausführlich (technische Details, Ursache, etc.)
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Sicherheitsbewertung

Ihre Einschätzung des Schweregrads:
☐ Kritisch (CVSS 9.0-10.0)
☐ Hoch (CVSS 7.0-8.9)
☐ Mittel (CVSS 4.0-6.9)
☐ Niedrig (CVSS 0.1-3.9)
☐ Keine (CVSS 0.0)

CVSS v4.0 Score (falls berechnet): _____
(z.B. "CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H")

Voraussetzungen für die Ausnutzung:
☐ Kein Nutzerzugriff erforderlich (Remote, unauthentifiziert)
☐ Netzwerkzugriff erforderlich
☐ Physischer Zugriff zum Gerät erforderlich
☐ Nutzerinteraktion erforderlich
☐ Entwickler-/Root-Zugriff erforderlich
☐ Spezielle Hardware erforderlich
☐ Sonstiges: _____

Mögliche Auswirkungen: (Mehrfachauswahl möglich)
☐ Datendiebstahl
☐ Systemkompromittierung
☐ Privilegieneskalation
☐ Denial of Service
☐ Umgehung von Sicherheitsmechanismen
☐ Manipulation von Daten
☐ Tracking/Überwachung
☐ Physische Geräteschäden
☐ Sonstiges: _____

Reproduktion

Ist die Schwachstelle reproduzierbar?
☐ Ja, zuverlässig (100%)
☐ Ja, meistens (>75%)
☐ Manchmal (25-75%)
☐ Selten (<25%)
☐ Nur einmal beobachtet

Schritt-für-Schritt Reproduktionsanleitung:
Bitte beschreiben Sie detailliert, wie die Schwachstelle reproduziert werden kann

1. _____

2. _____

3. _____

Proof of Concept (PoC):
☐ PoC-Code/Skript ist beigefügt
☐ PoC-Video ist beigefügt
☐ Screenshots sind beigefügt
☐ Detaillierte Anleitung (siehe oben)
☐ Kein PoC verfügbar

PoC-Code/Dateien: _____

Bitte fügen Sie Code-Snippets ein oder verlinken Sie auf sichere Weise (z.B. verschlüsselt)

[PoC-Code oder Link zu PoC-Dateien]

_____
_____

Entdeckungskontext

Wie wurde die Schwachstelle entdeckt?
☐ Manuelles Pentesting
☐ Automatisiertes Scanning/Fuzzing
☐ Code-Review
☐ Reverse Engineering
☐ Zufällig während normaler Nutzung
☐ Sonstiges: _____

Verwendete Tools/Methoden: _____
(z.B. "Burp Suite, Ghidra, Custom Python Script")

Zeitraum der Untersuchung: _____
(z.B. "3 Tage", "2 Wochen")

Haben Sie diese Schwachstelle bereits woanders gemeldet?
☐ Nein, nur bei Ihnen
☐ Ja, an: _____ (Datum: _____)

Zusätzliche Informationen

Gibt es bereits öffentliche Informationen zu dieser Schwachstelle?
☐ Nein
☐ Ja, siehe: _____

Ist Ihnen bekannt, ob diese Schwachstelle bereits aktiv ausgenutzt wird?
☐ Nein
☐ Ja, Details: _____
☐ Unbekannt

Vorschläge für Abhilfemaßnahmen: _____

Optional - falls Sie Ideen für Patches oder Mitigations haben [Ihre Vorschläge]

_____
_____
_____

Abhängigkeiten/Zusammenhänge: Steht diese Schwachstelle im Zusammenhang mit anderen Schwachstellen? Ist sie Teil einer Chain? [Ihre Anmerkungen hier]

_____
_____
_____
_____

Veröffentlichung & Zeitplan

Geplante öffentliche Veröffentlichung:
☐ Keine geplant
☐ Nach koordiniertem Disclosure mit Ihnen
☐ Nach fester Frist: _____ Tage (Standard: 90 Tage)
☐ Sofortige Veröffentlichung geplant (bitte begründen)

Grund für eventuelle Eile: _____
(Falls Sie aus bestimmten Gründen eine schnellere Veröffentlichung planen)

[Ihre Begründung hier]

_____
_____
_____
_____

Rechtliche Hinweise & Bestätigung

Bestätigung:

☐ Ich bestätige, dass ich diese Schwachstelle auf rechtmäßige Weise an einem eigenen Gerät oder mit ausdrücklicher Genehmigung entdeckt habe.

☐ Ich habe keine Daten anderer Nutzer eingesehen, kopiert oder verändert.

☐ Ich habe Ihre Richtlinien zur verantwortungsvollen Offenlegung gelesen und akzeptiere diese.

☐ Ich stimme zu, dass die Schwachstelle vertraulich behandelt wird, bis eine koordinierte Veröffentlichung vereinbart wurde.

Anhänge

Hochgeladene Dateien:
Bitte listen Sie alle beigefügten Dateien auf

- ☐ Screenshots
- ☐ Videos
- ☐ Log-Dateien
- ☐ PoC-Code
- ☐ Crash Dumps
- ☐ Sonstiges: _____

Hinweise zu Anhängen:
Sensible Daten bitte verschlüsseln (PGP empfohlen)

Vielen Dank für Ihren Beitrag zur Sicherheit unserer Produkte!

Nachdem Sie diesen Fragebogen ausgefüllt haben, senden Sie ihn bitte an:

security@isafe-mobile.com

Für sensible Informationen nutzen Sie bitte unseren PGP-Key: [PGP-Key]

Nur für interne Verwendung

(Dieser Bereich wird von unserem Security-Team ausgefüllt)

Ticket-ID: _____

Eingangsdatum: _____

Zugewiesener Analyst: _____

Verifizierungsstatus: ☐ Verifiziert ☐ In Prüfung ☐ Nicht reproduzierbar

Interner CVSS Score: _____

Priorität: ☐ P1 ☐ P2 ☐ P3 ☐ P4

Geplantes Patch-Release: _____