Vulnerability Disclosure Report – Questionnaire

Contact details

Name / Pseudonym *: _____
(May also be a handle/nickname)

Email address *: _____
(For communication during the process)

Alternative contact method: _____
(e.g. Signal, Telegram, PGP key)

Organisation/Affiliation: _____
(If you are conducting research on behalf of an organisation or company)

Would you like to be listed in our Hall of Fame?

☐ Yes, with name/handle: _____

☐ No, I'd prefer to remain anonymous

[* - Required field]

Product concerned

Product category: (Please select)

☐ Smartphone
☐ Tablet
☐ IoT device (Windows 11 IoT)
☐ Firmware/System software
☐ Mobile app
☐ Web service/backend
☐ Other: _____

Product name/model designation: _____
(e.g. "ModelX Pro", "TabletY 2024")

Firmware/software version _____:
(e.g. "Android 14.0.1 Build 20240115", "Windows 11 IoT LTSC 2024 v10.0.26100.2161")

Hardware revision (if applicable): _____
(e.g. "Rev 2.1", "Hardware ID: XYZ123")

Vulnerability details

Vulnerability title (max. 100 characters)

_____
_____
_____
_____
_____

Vulnerability type: (multiple selections possible)
☐ 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 vulnerability
☐ Firmware vulnerability
☐ Driver vulnerability
☐ Other: _____

Affected component:
☐ AOSP/Android system
☐ Custom firmware modifications
☐ Hardware/Bootloader
☐ Windows IoT System
☐ Custom drivers
☐ Kernel
☐ System app/service
☐ User app
☐ Network stack
☐ Miscellaneous: _____

Detailed description:
Please describe the vulnerability in detail (technical details, cause, etc.)

Security rating

Your assessment of the severity:
☐ Critical (CVSS 9.0–10.0)
☐ High (CVSS 7.0–8.9)
☐ Medium (CVSS 4.0–6.9)
☐ Low (CVSS 0.1–3.9)
☐ None (CVSS 0.0)

CVSS v4.0 score (if calculated): _____
(e.g. "CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H")

Exploitation requirements:
☐ No user access required (remote, unauthenticated)
☐ Network access required
☐ Physical access to the device required
☐ User interaction required
☐ Developer/root access required
☐ Special hardware required
☐ Other: _____

Possible consequences: (multiple selections possible)
☐ Data theft
☐ System compromise
☐ Privilege escalation
☐ Denial of service
☐ Circumvention of security mechanisms
☐ Data manipulation
☐ Tracking/monitoring
☐ Physical damage to devices
☐ Miscellaneous: _____

Reproduction

Is the vulnerability reproducible?
☐ Yes, reliably (100%)
☐ Yes, most of the time (>75%)
☐ Sometimes (25–75%)
☐ Rarely (<25%)
☐ Observed only once

Step-by-step instructions for reproducing the issue:
Please describe in detail how the vulnerability can be reproduced

1. _____

2. _____

3. _____

Proof of Concept (PoC):
☐ PoC code/script is attached
☐ PoC video is attached
☐ Screenshots are attached
☐ Detailed instructions (see above)
☐ No PoC available

PoC code/files: _____

Please paste code snippets or provide a secure link (e.g. encrypted) [PoC code or link to

PoC files]

_____
_____

Context of discovery

How was the vulnerability discovered?
☐ Manual penetration testing
☐ Automated scanning/fuzzing
☐ Code review
☐ Reverse engineering
☐ By chance during normal use
☐ Other: _____

Tools/methods used: _____
(e.g. 'Burp Suite, Ghidra, custom Python script')

Duration of the investigation: _____
(e.g. "3 days", "2 weeks")

Have you already reported this vulnerability elsewhere?
☐ No, only to you
☐ Yes, to: _____(Date: _____)

Additional information

Is there already any public information available about this vulnerability?
☐ No

☐ Yes, see: _____

Are you aware of whether this vulnerability is already being actively exploited?
☐ No
☐ Yes, details: _____
☐ Unknown

Suggested remedies: _____

Optional – if you have any ideas for patches or mitigations [Your suggestions]

_____
_____
_____

Dependencies/relationships: Is this vulnerability related to other vulnerabilities? Is it part of a chain? [Your comments here]

_____
_____
_____
_____

Publication & Timeline

Planned public disclosure:
☐ None planned
☐ Following coordinated disclosure with you
☐ After a fixed deadline: __Days (default: 90 days)
☐ Immediate publication planned (please give reasons)

Reason for any urgency: _____
(If you are planning an earlier publication for specific reasons) [Your reason

here]

_____
_____
_____
_____

Legal notices & confirmation

Confirmation:

☐ I confirm that I discovered this vulnerability lawfully on my own device or with express authorisation.

☐ I have not viewed, copied or altered any other users' data.

☐ I have read and accept your guidelines on responsible disclosure.

☐ I agree that the vulnerability will be treated as confidential until a coordinated disclosure has been agreed.

Attachments Uploaded

files:
Please list all attached files

- ☐ Screenshots
- ☐ Videos
- ☐ Log files
- ☐ PoC code
- ☐ Crash dumps
- ☐ Other: _____

Notes on attachments:
Please encrypt any sensitive data (PGP recommended)

Thank you very much for helping to ensure the security of our products!

Once you have completed this questionnaire, please send it to:

security@isafe-mobile.com

For sensitive information, please use our PGP key: [PGP key]

For internal use only

(This section is to be completed by our security team) Ticket

ID: _____

Date received: _____

Assigned analyst: _____

Verification status: ☐ Verified ☐ Under review ☐ Unreproducible

Internal CVSS score: _____

Priority: ☐ P1 ☐ P2 ☐ P3 ☐ P4

Planned patch release: _____