




SOZO® PENETRATION / INFORMATION SECURITY TESTING SUMMARY

ImpediMed Limited
ABN 65 089 705 144
Tel: +61 (0)7 3860 3700
Fax: +61 (0)7 3260 1225
Free Call: 1800 638 477
Email: enquiries@impedimed.com

PM-123
Rev. F
Dated 17 MAY 2021

	TITLE: SOZO PENETRATION / INFORMATION SECURITY TESTING SUMMARY	
	Doc. No. PM-123	Rev. F

1 Introduction

ImpediMed is a medical device company that designs and produces medical device hardware and software. The company is committed to quality as evidenced by its certified processes to EN ISO 13485 and software is produced to IEC 62304:2006. The company is also committed to security and is HITRUST Certified. The company conforms with EN ISO 14971 for its risk assessment and management of medical device design and production.

This document outlines the Penetration / Information Security Testing Summary as performed by our Security Penetration Test partner – CENSUS S.A. on SOZO v4.0 App / MySOZO software. The penetration testing occurred in April 2021.

2 Penetration Testing Role in SW Development

ImpediMed maintains robust processes that require continuous improvement to our products and services. The security penetration test is highly valued by ImpediMed as one way to identify security risks and thus lead to improvements in the security of our software solution. Our general intent is to address medium and high security risks in the timeliest fashion, typically in the next Software release (if practical) as has been demonstrated in the latest release of software v4.0. During software development, the software team works with our security test partner to develop secure functionality. Upon major software releases, penetration testing will be conducted and the process repeated.

3 Summary of Results

ImpediMed has adopted the policy of not publishing detailed penetration test results. To do so is imprudent from a security perspective as the information could be advantageous to a potential hacker.

When conducting the penetration testing, Census categorized security risk into high / medium / low categories based on the following criteria: It should be noted that these risk categories are based on functionality and security of the system and are not based on patient or health risk.

impedimed	TITLE: SOZO PENETRATION / INFORMATION SECURITY TESTING SUMMARY	
	Doc. No. PM-123	Rev. F

- **High risk issues:** these are *release-critical* issues, that may allow an attacker to compromise the security of the system
- **Medium risk issues:** these are *release-critical* issues, that may allow an attacker to compromise partly the security of the system (e.g. create a denial of service condition)
- **Low risk issues:** these are security issues that do not pose a serious threat and are sometimes dependent on the exploitation of other issues

The number of risks identified in version **4.0** were significantly reduced from version 3.0.0. **Version 4.0 maintains zero high and medium risks.** Version 4.0 has significant feature updates including investment into security and privacy which eliminated many potential risks.

Summary of risk evolution from 3.0.0 to **4.0**:

Risk Category	# of Risks identified in 3.0.0	# of Risks identified in v3.1.0	# of Risks identified in v4.0
High	0	0	0
Medium	7	1	0
Low	13	26	26

The *one* remaining medium level risk that had been previously identified in the version **3.1.0** software has been mitigated. ImpediMed has reviewed the *low risks (most of which can be mitigated by the customer's MDM and Browser policies)* and has accepted them with the commitment to continue to improve upon them in the future software releases *where possible*.

4 Penetration Testing Summary Letter from CENSUS



May 6th, 2021

Re: SOZO Software v4.0.0 Security Assessment and Penetration Testing Report Summary

To whom it may concern,

We would like to inform you that during the period between March 16th and April 1st, 2021, CENSUS conducted a black-box security assessment to a release candidate of SOZO Software version 4.0.0 This release included the following components:

- SOZO App v4.0.0 for Android
- SOZO App v4.0.0 for iOS
- SOZO Portal (SOZO Web Frontend) v4.0.0
- SOZO Cloud API v4.0.0
- BIS Firmware v4.0.0

During this assessment, CENSUS security consultants performed a black-box security testing on a test cloud environment and test app build provided by Impedimed. Adequate test data and user accounts were also provided to exercise all user roles and application functionalities.

The testing methodology that was used, is based on best practices described in the latest version of the OWASP Testing Guide, the OWASP Application Security Verification Standard and the NIST Technical Guide to Information Security Testing and Assessment, and allows for a thorough examination of all aspects of applications including:

- Configuration and Deployment Management issues
- Identity management issues
- Authentication
- Authorization
- Access control
- Session management
- Data validation
- Error handling
- Communication & protocol security

CENSUS S.A.
I. Gkoura 16, 54352,
Thessaloniki, Greece.
T. +30 2310 947 287
F. +30 2311 241 451
E. info@census-labs.com
www.census-labs.com

- Weak Cryptography
- Business logic errors
- Client-side issues
- Handling of sensitive information
- Unsafe use of third-party software

More information about the assessment services of CENSUS and its leading IT Security research can be found at <https://census-labs.com>.

The SOZO Software security assessment identified one (1) HIGH-risk issue, two (2) MEDIUM-risk issues and twenty-six (26) LOW-risk issues. Twenty (20) INFORMATIONAL findings were reported, which constitute no risk to the users of the software, but whose mitigation would further improve the security of the SOZO platform.

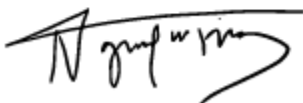
Impedimed proceeded to actions of issue remediation and the April 29th, 2021 issue retesting session CENSUS determined that:

- All HIGH and MEDIUM-risk issues were sufficiently addressed.
- The twenty-six (26) LOW-risk issues remained OPEN.
- The twenty (20) INFORMATIONAL findings remained OPEN.

It must be noted that most of the new issues identified in the assessment of April 29th, 2021 concerned vulnerabilities that could only be exploited in environments where a malicious insider (e.g. a clinician or clinic administrator) would be operating. Furthermore, the software code base was found to employ a number of secure development best practices that made the code immune to common software vulnerabilities, such as SQL injection and Cross-Site Scripting.

CENSUS remains available for any further information required regarding the above security assessment work.

Sincerely,



Nikolaos Tsagkarakis
CEO