SIB Swiss Institute of Bioinformatics

Recheck Security Assessment BioMedIT 2026

Version:	v1.0
Project Number:	91369
Date of Delivery:	July 23rd, 2026

Compass Security Schweiz AG, Werkstrasse 20, CH-8640 Rapperswil
T +41 58 510 36 00, team.csch@compass-security.com, www.compass-security.com

Executive Summary

In November and December 2025, Compass Security Schweiz AG (Compass) conducted a security assessment of the BioMedIT infrastructure, including all the nodes hosted by Uni Basel, Uni Lausanne and ETH Zürich, as well as the central services of the BioMedIT network. In June 2026 Compass performed a recheck of all high and critical vulnerabilities identified in the initial assessment. This document is intended to provide a high-level summary of the assessment results after the recheck. Further details have been reported to BioMedIT and the affected organizations in separate documents.

Scope

The performed tests including the systems in scope and their timeline are listed in the following table:

Target	Date	Effort
Central Services ▪ External Penetration Test ▪ IT Infrastructure Review ▪ Manual Hacking BioMedIT Portal & IdP Integration ▪ Manual Hacking Data Import	03.11.2025-14.11.2025	8.00 PD
Uni Basel (sciCORE) ▪ IT Infrastructure Review ▪ External Penetration Test ▪ B-Space Segregation & Exfiltration	03.11.2025-11.11.2025	5.00 PD
Uni Lausanne (SENSA) ▪ IT Infrastructure Review ▪ External Penetration Test ▪ B-Space Segregation & Exfiltration	03.12.2025-18.12.2025	6.50 PD
ETH Zürich (LeoMedIT) ▪ IT Infrastructure Review ▪ External Penetration Test ▪ B-Space Segregation & Exfiltration	08.12.2025-12.12.2025	4.50 PD
Recheck All high and critical vulnerabilities from the initial assessment. This includes vulnerabilities within all of the above organizations.	29.06.2026-30.06.2026	1.00 PD

The statements made in this document are only applicable to the exact versions and/or dates listed above.

Procedures

The initial assessment consisted of a security assessment of each organization involved in the BioMedIT network. This included the infrastructure at central services, as well as the B-Space infrastructure maintained by the different nodes of the BioMedIT network.

For the infrastructure at central services this included three components. First, externally exposed services were assessed from the perspective of an anonymous attacker. Then the BioMedIT portal was assessed using the perspective of both an anonymous attacker as well as an attacker having access to the application as an authenticated user. Lastly, the data import process using SETT was assessed with the permissions of a data provider importing data to a B-Space.

For the nodes maintaining the different B-Space infrastructure the following approach was used to assess each of these: The external infrastructure was assessed from the perspective of an anonymous attacker, whose source IP is whitelisted in a B-Space. The internal infrastructure was assessed as a regular B-Space user.

Additionally, for all organizations the whole infrastructure was reviewed conceptually based on an interview with the people responsible for the corresponding organization.

The recheck only considered the critical and high rated vulnerabilities and a customer selected set of medium rated vulnerabilities identified in the initial assessment. Other medium or low rated vulnerabilities were not assessed. The recheck of these vulnerabilities was conducted using the same approach as in the initial assessment.

Weakness Rating

Compass groups the findings into four categories: low, medium, high and critical. The ratings are based on their intrinsic technical properties and are not a risk score. Other factors such as a threat actor's motivation or financial loss incurred by a successful exploitation of a vulnerability have not necessarily been considered.

Results

After the recheck, no critical or high rated vulnerabilities remain. All organizations implemented proper remediation of the previously critical or high rated vulnerabilities. Thus, the infrastructure of the BioMedIT network presents itself with a robust security posture.

At central services security relevant checks are implemented properly, so that unauthorized access to the infrastructure at central services, including externally exposed infrastructure, the BioMedIT portal, or the data import process using SETT is restricted to authorized users.

Similarly, the B-Space infrastructure maintained by all nodes presents itself with a robust security posture. Relevant security mechanisms are in place and restrict unauthorized access within the external and internal B-Space infrastructure.

The remaining vulnerabilities have only a severity of medium or low and do not present direct exploitable threats. Compass Security recommends addressing these in the future to improve the security posture even further.

About

Compass Security Schweiz AG is a Swiss IT security company specializing in providing tailored high-quality attack simulations, security assessments and forensic investigations to customers. Founded in 1999, Compass has over 25 years of experience working on national and international projects with Fortune 500 companies, small and medium-sized companies, as well as with start-ups operating in the financial, medical, industrial, and pharmaceutical industries. The diverse training and specializations of our security analysts, as well as close cooperation with leading Swiss universities, ensure that our analysts are always informed about the latest developments in the security industry.