nSEC/Resilience

IT Security | IT Performance

Statement of results

Penetration Test

EasyConf Connect

MVI Audiovisual

Version 1.0, January 21st, 2025

Context and objective of this document

MVI AudioVisual offers the meeting management tool EasyConf Connect. EasyConf Connect enables hybrid meetings, enabling users to participate in remote meetings/rooms, seeing and hearing all participants. Meetings can be initiated via client applications from various client devices using various operating systems like iOS, Windows and Android.

To gain insight in the security aspects of EasyConf Connect MVI AudioVisual mandated nSEC/Resilience to perform a penetration test on the EasyConf Connect ecosystem.

This document serves as a summary of the executed penetration test on e-health platform. The document is concluded with quality statement on the application(s) based on the outcomes of the test.

Description of the executed test

The penetration test was executed in October 2024 by a team of 2 nSEC/Resilience security consultants, holding at least CEH, supplemented with either SANS GPEN and/or Advanced Penetration Testing certifications like xWPT or OSCP.

The infrastructural elements of this penetration tests were performed in line with the industry standard methodology PTES. For the application-level tests, the OWASP (API) top 10 and the OWASP WSTG standards were used. The penetration test was executed as a grey-box penetration test.

Attack surface (areas of the information system that an attacker or security evaluator choose to initiate an attack) for the assignment is defined and limited to:

- The EasyConf Connect ecosystem, being:
    - *EasyConf Connect Server (Redistribution server)* and the *MVI local server software*, both network and application level;
    - *EasyConf Connect client applications*, both network and application level.

During the penetration test an extensive exploration was performed on as well network-, infra- and application level. The results of the exploration were used in the exploitation phase.

During the exploitation phase many validations were performed, in line with the PTES and OWASP WSTG standards. For the application-level tests at least the OWASP top 10 vulnerabilities were covered.

Statement of results and quality statement

During the penetration test a few recommendations were formulated via findings to secure and improve the security aspects of EasyConf Connect. These recommendations were picked up by MVI Audiovisual. After releasing several fixes a retest was performed. After the performed retest only a few findings with low severity remain. For the low severity findings, there is no direct urgency to fix.

Although each penetration test is a security snapshot of a system in a specific moment in time, and periodical penetration testing is always advised to ensure continued security of EasyConf Connect, nSEC/Resilience states that the results of the executed tests show that, from an external point of view (view from client perspective), the considered security aspects of the functionality as offered in EasyConf Connect are of a good security level.