



Thick Client Application Security Audit Certificate

Certificate No: IMS/2026-2027/ 0099

Audit Details

Audit Firm	:	Imperium Solutions 401, 4th Floor, Maruti Bhavan, Ram Maruti Road, Thane (W) 400601 www.imperiumsolutions.com email: info@imperiumsolutions.com
CertIN Empanelment Reference	:	3(15)/2004-CERT-In (Vol.XIV) Dated 08.10.2025
Client Name	:	Elektro Labs
Scope of activity	:	Thick Client Application Vulnerability Assessment and Penetration Testing (VAPT)
Application Name	:	ElektrolabsHUB
Tested Application	:	ElektrolabsHUB.msi
Audit Duration	:	5 th May 2026 – 14 th May 2026
SHA256 Hash	:	9e71b18701faaa579f85e0c2c2023079e219abcc64ea4d39c950dab877938ca8
Audit Methodology	:	OWASP, SANS, Cert-IN Advisory, OSSTMM, PTES, ISSAF

Auditor Details	:	Mr. Om Pagar
Certificate Issue Date	:	14 th May 2026
Certificate Validity	:	This certificate is valid till there are no changes in the application

Conclusion

The Elektrolabs HUB Thick Client Application was in the scope of the activity. It was observed that two low vulnerabilities identified during the audit have been taken as exceptions by ELEKTRO LABS.

Sr.no	Vulnerability Name	Severity	Final Status
1	Authenticode is Missing	Low	Exception
2	Unsigned Code	Low	Exception

The application can be hosted in the production environment after implementing the compensatory controls.

General Recommendations

Production Hosting Environment – Thick Client Application

1. Deploy a Thick Client Application Firewall ahead of your application facing the Internet and allow only relevant traffic to flow to your web server.
2. Fine tune the firewall rules such that only specific ports and IP addresses are allowed access to your application.
3. Enable, capture and retain application logs so as to be able to trace a security incident, in case it becomes necessary to do so.
4. Utilise services of 3rd party vendors to check for malicious activities like web defacement, etc.
5. Ensure that the Operating system, database and application is hardened.
6. Ensure that the Operating Systems, Database and applications is the latest stable version.
7. Application should undergo security testing annually or whenever any changes are implemented in the application functionality, whichever is earlier.

8. Ensure that all vulnerabilities, irrespective of their criticality, are resolved asap.

For Imperium Solutions,

Mr. Jude Dcosta

Dated: 14th May 2026