To Kramer Electronics Ltd January 2018

Security Testing Summary

General

Public and private companies depend on communications and information systems to successfully fulfill their business goals. These systems are subject to threats that can harm the company, its assets and employees by exploiting known vulnerabilities and those of unknown origin and thus jeopardize the confidentiality, integrity and availability of information stored, processed or transmitted by these systems. Threats to these systems may include purposeful attacks, disruptions, environmental, human/machine errors and structural failures. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of the organization.

Madsec Security Ltd. (hereafter called "Madsec") is equipped with rich implementation experience in risk management, across industries and multiple global databases. Madsec information-security-consulting team provides evaluation, planning and implementation of information security consulting that are aligned to organizational business strategy, to assist organizations in effectively using and protecting their critical data assets. Madsec team carries out risk surveys based on led methodology and international standards emphasis on NIST[1] 800-53 Rev.4. And OWASP 2017

Kramer Electronics Ltd. hired the services of Madsec to carry out information-security risk Tests. In the month of January 2018, Madsec performed Penetration Testing routine that was held throughout review of "Kramer Control Platform" including both application and infrastructure of the platform.

Purpose

To introduce company stakeholders with existing vulnerabilities, based on commonly known attacking-scenarios. To provide with recommendations, as to the risks of information security systems and existing processes evaluation.

Scope of Risk Penetration Testing

Penetration testing of company application and infrastructure. The following components were reviewed:

- Code Injections
- Broken Authentication and Session Management (XSS)
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Invalidated Redirects and Forwards
- Network topology
- Infrastructure vulnerabilities assessment

Current Status of the Application

Based on the testing result of “Kramer Control Platform” on January 2018, Madsec confirms that no critical or high-risk vulnerabilities were found at the period testing time.

Best Regards

דורון סיון

Doron Sivan, CEO

מדסק סקיוריטי בע״מ