LEGAL SERVICES CORPORATION
OFFICE OF INSPECTOR GENERAL
(LSC OIG)

LSC OIG Information Technology Vulnerability Assessment

Summary of Recommendations

Date: May 24, 2022

Prepared by

SECURICON

Information Security Solutions

Executive Summary

The Legal Services Corporation Office of Inspector General (LSC OIG) contracted with Securicon LLC (Securicon) to perform vulnerability scans on grantee information technology (IT) systems. Securicon scanned and assessed the network security of six grantee sites over a 10-month period. Based on an OIG Risk Assessment four grantees were selected by LSC OIG while two grantees requested the scan. The grantees were geographically dispersed and differed in the number of sites and network architecture design.

A vulnerability assessment provides grantee management and system and security administrators visibility to potential issues in the target network environment. These vulnerabilities may provide malicious actors an ability to exploit, compromise, modify or damage grantee data, information systems, or reputation. Identifying grantee information system vulnerabilities is essential to address known risks as part of a risk management program. The objective of the vulnerability assessment was to determine if the grantees' networks have vulnerabilities that can be exploited to compromise the integrity of the system or data or allow the theft and unauthorized manipulation of data and resources.

The assessments included vulnerability analysis to identify technical and procedural weaknesses that create risks to grantees' information technology systems. During the assessment, network systems were evaluated, and configurations were reviewed. Information collected was analyzed to identify vulnerabilities and issues that might affect grantees' overall information security posture at the point of time the assessment was conducted.

Findings and observations identified during each grantee site's remote assessment pertain only to hosts scanned at the time of the assessments. The security posture of all grantee sites was like those typically found in small- to mid-size businesses. Of the assessments performed, grantee sites generally did not present a high level of risk of exposure from outside their networks. However, there were several critical and high-level vulnerabilities found during the internal assessment of grantee networks.

The assessment resulted in issuance of six assessment reports which were shared with the individual grantees. This summary report lists recommendations and industry best practices for grantees to follow that mitigate vulnerabilities and strengthen network security.

Near Term or Tactical Recommendations

Tactical recommendations are short-term, and intended to immediately improve a grantee's security posture, if implemented. Tactical recommendations can also be thought of as "quick wins" requiring minimal cost, resources, or effort to implement. Tactical recommendations support strategic or long-term recommendations whenever possible.

The recommendations are:

1. At minimum, apply operating system and software updates on all affected systems to include patches for "critical" severity vulnerabilities.
2. Update and/or patch third party firmware and software. If the systems cannot be patched due to vendor constraints, enable a host-based firewall to block or filter connections to affected services. Segment network boundaries using a firewall or router and apply firewall rules or Access Control Lists to allow or deny traffic between zones as required.
3. When possible, remove unnecessary or unsupported software.
4. Develop and maintain an approved port, protocols, and services whitelist and close any undocumented open ports to significantly reduce grantee attack surface.

Long Term or Strategic Recommendations

Strategic recommendations define longer term initiatives. The goal is to prevent identified vulnerabilities from recurring. These initiatives may need to be addressed through formal security engineering efforts and may require substantial resources, budget, and time to implement.

The recommendations are:

1. Implement a vulnerability scanning system which can securely and routinely conduct authenticated scans and report on all grantee IT assets. Do not rely on host-based security tools or segmentation to obscure vulnerabilities (e.g., using host-based firewalls to hide operating system service vulnerabilities).
2. Implement a comprehensive patch management program to apply all available patches, firmware, and software updates. To prevent downtime or a negative impact on business operations, grantees should create a test and evaluation network which includes similar systems found in production

networks. Patches should be installed first in this environment to test for negative impact on systems and applications before installing the updates on production hosts. Alternatively, patches and updates may be scheduled outside of business hours to minimize business interruptions.

3. Ensure that all communications at the external managed interfaces, including cloud and/or publicly available system components, and at key internal managed interfaces, are properly monitored in accordance with the organization's overall security architecture.
4. Consider researching and employing modern zero-trust architectures and controls in line with current and emerging industry standards. Zero-trust acknowledges the need to dissolve the reliance on a singular authentication and control boundary to effectively mitigate risks.
5. Conduct routine manual and automated device inventories, seeking to isolate and interrogate rogue devices.
6. Implement network segmentation to separate assets according to their risk or level of control. For example, move IP phones into a network separate from servers or desktop systems. Grantees should seek to establish clear physical and logical separation between static authorized systems and transitory non-grantee controlled remote systems and devices (e.g., personally owned digital devices).
7. Establish clear physical and logical separation between static authorized systems and transitory non-grantee controlled remote systems and devices (e.g., personally owned digital devices).