iterasec

Securing NDA Security company's AWS Single-Tenant Deployments

Client:
NDA Security company

Industry:
Network Security and Infrastructure

Company Size:
300+ Employees

Services Used:
Penetration Testing, Secure Code Review, AWS Security Audit

Client

A Security company specialized in advanced solutions for network security, providing both software and hardware products designed to protect complex enterprise environments. Their offerings enabled organizations to gain enhanced visibility and control over their networks, helping them effectively manage threats and vulnerabilities. With a strong technical team and a focus on adaptability, this security company supported a variety of industries in meeting evolving security challenges.

Background

As Security company expanded its client base, the demand for a single-tenant version of its core product grew significantly. Each customer required a strictly isolated environment to ensure their proprietary data and internal processes remained confidential. To meet the needs of these clients, a Security company deployed its product and underlying infrastructure on AWS. Recognizing the complexity of this setup and the potential risks associated with cloud-based solutions, They partnered with Iterasec to perform a thorough security evaluation.

The Challenge

A Security company faced several key concerns as they embarked on providing single-tenant deployments:

- **Large-Scale Product and Infrastructure:**
  Their flagship solution — complete with multiple web applications, REST APIs, and an Appliance Web Admin — was extensively hosted on AWS. Ensuring airtight security across this broad environment was paramount.
- **High-Stakes Vulnerabilities:**
  Given company's reputation and the critical nature of their product, any undiscovered high-severity vulnerabilities (such as Remote Code Execution or Privilege Escalation) could profoundly impact their credibility and the confidentiality of client data.
- **Comprehensive Testing Needs:**
  The project demanded a multi-faceted approach, encompassing penetration testing of the software solution, AWS infrastructure audit, and in-depth source code analysis, reverse engineering, and dependencies management review.

The Solution

Iterasec designed and executed a comprehensive security assessment over the course of six weeks, focusing on two primary pillars: software penetration testing and an AWS security audit.

Scope Definition and White-Box Testing

- **RESTful and SOAP APIs:**
  Assessed both RESTful and SOAP APIs for secure authentication and authorization mechanisms, investigated potential code injection points, and looked for complex business logic flaws.
- **Appliance Web Admin:**
  Investigated administrative functionalities for privilege escalation risks.
- **Reverse Collector:**
  Conducted specialized analysis to identify vulnerabilities in data collection components with the focus on data confidentiality and integrity, as well as on the component's availability.
- **SaaS Infrastructure:**
  Performed a thorough evaluation of the AWS environment, identifying misconfigurations, insecure network setups, and possible attack vectors.

Secure Code Review and Reverse Engineering

- **Reviewed critical modules and libraries to spot weaknesses at the code level.**
- **Verified third-party dependencies to prevent known vulnerabilities from affecting core functionality.**
- **Validated encryption mechanisms in both custom web-applications and 3rd-party services.**

Firewall & Network Assurance

- **Evaluated network segmentation, AWS Security Groups and NACL configurations.**
- **Provided insights for the AWS ELB configurations to prevent complex attacks on discrepancies in HTTP parsers, e.g. HTTP Request Smuggling.**
- **Recommended best practices for continuous monitoring and policy management.**

Immediate Reporting of High-Severity Findings

- **Established regular communication channels and immediate alerts for critical issues.**
- **Provided detailed technical guidance to company's developers and DevOps teams, ensuring rapid remediation of high-severity vulnerabilities. This included several in-depth Zoom sessions with their architects to discuss the Remote Code Execution (RCE) issue in the Reverse Collector and collaboratively develop a comprehensive mitigation strategy, reinforcing the overall security posture.**

The Outcome

- **Identification of 31 Security Findings:**
  - Five High-Severity Issues: Included Remote Code Execution, privilege escalation in administrative functionalities, and multiple SQL injection vectors.
  - Denial-of-Service Vulnerabilities: Discovered potential DoS exploits through business logic flaws, impacting critical areas like Global Trends and Regexp Test functionality. Such attacks posed a significant threat to system availability—an essential requirement for any security monitoring solution.
  - Multiple AWS Misconfigurations: Addressed numerous security misconfigurations in core AWS services, including overprivileged IAM principals, improper data protection settings in S3, lax NACLs and HTTP request validation settings, and insecure KMS key rotation practices.
- **Swift Remediation and Retest**
  - A Security company promptly addressed all high-severity findings, implementing fixes guided by Iterasec recommendations.
  - A subsequent retest confirmed that the most impactful vulnerabilities had been effectively resolved.
- **Enhanced Overall Security Posture**
  - Strengthened defenses in both the software and AWS infrastructure, aligning with industry best practices.
  - Guided towards secure-by-default cloud configurations with AWS Config.
  - Developed a clearer roadmap for ongoing improvements in dependency management, network segmentation, and secure software development.
- **Improved Communication and Collaboration**
  - Frequent, in-depth Zoom sessions with Skybox Security's team allowed for detailed discussions on critical issues, notably the RCE in the Reverse Collector, ensuring swift and effective mitigation strategies.
  - The collaboration established a solid framework for future audits, ensuring continuous advancement of security measures.

Conclusion

Iterasec extensive penetration testing, Secure Code Review, and AWS security audit empowered a Security company to reinforce the reliability of its single-tenant solution. By identifying critical vulnerabilities, guiding swift remediation efforts, and enhancing overall security practices, Iterasec helped them uphold its reputation as a trusted leader in network security. This partnership underscores Iterasec commitment to delivering tailored, in-depth cybersecurity services that drive lasting resilience and customer confidence.