AppOmni

Rules of Engagement for Research at AppOmni

Purpose

The mission of AO Labs is to identify misconfigurations and related vulnerabilities in SaaS applications used by the customers organization or other organizations.

This policy provides security researchers at AppOmni with clear guidelines for the following activities:

- Conducting misconfiguration, attack vector, and incident vulnerability discovery activities directed SaaS applications of interest within AppOmni's product strategy
- Approved high-level Tactics, Techniques, and Procedures (TTPs) for use during the conduct of scoped research activities.

Scope

- This policy applies to all employees and representatives of AppOmni when conducting research activities on SaaS applications using company assets aligned to their role and responsibilities at AppOmni.
- Research conducted as part of employment with AppOmni is considered intellectual property of the company under applicable state laws. This includes any misconfiguration research, tools, exploits, techniques, documentation, reports, and materials developed during research activities or while using company resources.
- Employees and representatives may not disclose or publish any company intellectual property without express written consent of AppOmni management.
- This policy does not apply to general technical knowledge and skills gained during employment that do not constitute intellectual property of the company under relevant laws.
- Employees and representatives should properly classify research output and activities as belonging to AppOmni or not based on applicable laws. When uncertain, consult management.
- Violations of this policy, including unauthorized release of AppOmni intellectual property, may result in disciplinary action up to termination of employment or contracts.

The intent is to protect AppOmni's proprietary research while allowing researchers to build general technical knowledge. Employees and representatives should consult management if unsure whether research activities or output constitute company intellectual property under the applicable laws.

Principles

- First, do no harm. Our foremost priority is the absolute safety and well-being of our customers. We ensure at all times that no action or inaction on our part puts our customers in any form of risk or danger.
- Provide the diagnosis with the cure. Under no circumstances do we highlight a risk without simultaneously providing a clear and practical mitigation strategy.
- Focus on understanding who holds the ability and the responsibility to take necessary action.

- During the process of releasing any findings, we take it upon ourselves to ensure that all real-world edge cases, including those that exist within customer environments, are thoroughly considered and accounted for. This diligent approach allows us to preemptively address potential issues.
- We adhere to the Traffic Light Protocol (TLP) classification system from the Critical Infrastructure Security Agency (CISA), which is widely accepted and used by many Information Sharing and Analysis Centers (ISACs).

Classifying Findings: Defining and Distinguishing between Misconfigurations and Vulnerabilities

Misconfigurations

A misconfiguration is a risk or security gap that is the result of a SaaS application setting or configuration that is under the control of the user. Specific configurations may result in security risks and are usually from an improper or incorrect use of a platform. In these scenarios, customers have the ability to mitigate this risk themselves by adjusting a configuration or control in the application.

- This is the primary focus of our research.
- We promptly publish information about misconfigurations to partners, customers, and then publicly.
- We highlight these in ISACs.

Vulnerabilities

A vulnerability is a weakness, flaw, or error found within a SaaS vendor's software or platform that creates a security risk and has the potential to be exploited. Vulnerabilities require changes by a vendor, and relevant to SaaS applications, end-users or customers of a SaaS service do not have the ability to mitigate the vulnerability themselves. The user does not have the ability to mitigate this risk themselves, and it is the vendor's responsibility to address and mitigate it.

- This is an incidental outcome of our research, not a deliberate focus.
- We follow a strict protocol of disclosing any identified vulnerabilities through the appropriate official channels.
- We also take the step to privately disclose these vulnerabilities to ISACs, with a classification of TLP:AMBER+STRICT, to ensure they are aware and can take necessary action.
- The criteria for publishing vulnerabilities are:
  - The vendor has successfully resolved the identified vulnerability.
  - The vendor has been unresponsive for a period of time specified in the respective vendor's vulnerability disclosure policy's specified period.
  - AppOmni has direct evidence of the vulnerability being exploited within customer environments.

Link to disclosure process.

Operating Rules

- Our research activities mainly focus on detecting misconfigurations, improper settings, and related vulnerabilities in SaaS applications. In line with AppOmni Lab's mission to safeguard AppOmni's customers and push the envelope in SaaS security, researchers have the freedom to delve into other areas pertinent to SaaS security.
- Research activities must be conducted in accordance with existing partnership and vendor agreements.
- Researchers may only target SaaS applications and associated infrastructure, such as APIs and databases, that are owned and provided by an agreeing prospect, customer, or partner, or independently acquired environment. Testing third-party SaaS applications or infrastructure requires explicit written authorization from the application owner.
- Researchers must avoid accessing or modifying any sensitive customer data stored within SaaS applications, including personal information, financial data, or other confidential business data. Any customer data discovery during testing must be unintentional and minimized.

- Testing should never degrade the confidentiality, integrity or availability of the SaaS applications. This includes not conducting denial of service attacks, excessive scraping, injecting malicious content, or other activities that could harm the application.
- Researchers may only use lawfully obtained credentials for logging into SaaS applications. Testing must rely solely on identifying and exploiting misconfigured access controls and authentication schemes.
- Researchers should identify monitoring and detection capabilities that mitigate a vulnerability or misconfiguration finding, and implement, or work with an implementation team, to incorporate said capabilities into the product.
- All discovered misconfigurations, vulnerabilities, and associated risks must be promptly disclosed to the appropriate contacts at the client organization through responsible disclosure practices.
- Researchers must comply with responsible disclosure timelines dictated by the client organization before publicly releasing any research, whitepapers, or presentations related to the testing.
- When conducting research, researchers must adhere to AppOmni standards, values, ethics policies, and applicable laws. Activities should reflect positively on the organization.

Limitations

The goal of these limitations is to ensure research activities do not introduce undue risk to the client organization by restricting high-risk testing methods and scope. Limitations help maintain safety and prevent activities that could have unintended business impacts without proper coordination.

- Denial of service testing is prohibited under this policy. This includes flooding applications with traffic, overwhelming databases with requests, leveraging application flaws to crash services, and any other activities that could interrupt availability and access to the SaaS applications.
- Exploitability testing, which involves leveraging misconfigurations to demonstrate compromise of data or systems, is only permitted with explicit written authorization from the client. This helps ensure destructive or risky exploit testing is not conducted without approval.
- No physical penetration testing is allowed, including attempts to gain physical access to facilities, compromise badging systems, tailgate employees, retrieve documents from mailrooms, investigate trash, and any other unauthorized physical activities.
- By default, all testing must be conducted safely against non-production systems like development, test, and staging environments. Launching research activities against production systems containing live customer data and workloads introduces significant risk and liability. Explicit written authorization must be granted before targeting any production systems or data.

Legal / Authorization

- AppOmni researchers must adhere to organizational policies, values, ethics, and applicable laws at all times. This policy has been reviewed and approved by AppOmni Executives on November 2023 to ensure research activities are conducted responsibly.

TLP Classification Levels

TLP Level	Definition
TLP:CLEAR	This information is publicly available and can be shared with anyone.
TLP:GREEN	This information is sensitive but not confidential. It can be shared with a limited group of people who have a need to know.
TLP:AMBER	This information is confidential but can be shared with members of the same organization and its clients on a need-to-know basis to protect the organization and its clients and prevent further harm.
TLP:AMBER +STRICT	This information is highly confidential and should only be shared with a small group of people within the organization on a need-to-know basis to protect the organization and prevent further harm.
TLP:RED	This information is highly confidential and should only be shared with a very small group of people who have an absolute need to know.