WSO2 security commitment for on-premises customers

WSO2 is committed to ensuring that industry best practices regarding security standards and mechanisms are rigorously applied to our processes. Below are WSO2's security commitments to its on-premises customers, covering the type of data we collate and how such data is used, such as the security of product development, design, coding testing, etc.

Data processed by WSO2

- WSO2 only collects limited personally identifiable information (PII), such as full name, email address, phone number(s), and billing information, to provide support services and for billing purposes, per the WSO2 Privacy Policy.
- During the engagement with the customer, the WSO2 team would encounter limited information regarding the customer's requirements and environments to assist in the implementation and support-related matters through the official WSO2 support system and the official SFTP server. This information would be kept confidential.
- While providing enterprise support services, WSO2 may request logs, dumps, and configurations related to WSO2 products. However, WSO2 recommends sanitizing these artifacts before sharing.
- WSO2 does not require access to the customer's environment to provide support services.
- WSO2 updates service collects information regarding the product, product version, last applied update level, applied date, and customer email to validate subscriptions and send customer updates and notifications.

Secure Software Development Process

WSO2 has a well-defined Secure Software Development Process, which details how we incorporate security aspects into our product development process.

Security of product design

Security by design approach is followed within WSO2 for each new development initiative. It is conducted to identify the relevant security endpoints and trust boundaries to minimize the product vulnerabilities and reduce the attack surface through the product designing phase.

Secure coding and reviews

- WSO2 engineers adhere to the WSO2 Secure Engineering Guideline when doing engineering tasks. This guideline provides technical guidance on addressing OWASP's top 10 application security risks and additional security guidelines related to WSO2 Secure Development processes.
- WSO2 uses GitHub as our source code repository system. Source codes of products are available to the public in our GitHub organization for anyone to review and report security issues.

- Mandatory peer code reviews are performed before any change is added to the code base to identify security deficiencies.
- When a 3rd party dependency is introduced to the WSO2 product, WSO2 engineers and the Security and Compliance team will assess the security of such dependencies. Approved dependencies are added and reviewed as part of Third Party Dependency Analysis.

Security testing

- WSO2 ensures mandatory security checks are performed before releasing a new product version.
- WSO2 conducts mandatory product security assessments **during product release cycles** under three categories. Static Code Analysis, Software Composition Analysis, and Dynamic Analysis.
    - For Static Application Security Testing (SAST), we utilize the Find Security Bugs plugin, the Spotbugs plugin, Super-Linter, GoSec, and Veracode Static Analysis.
    - For Dynamic Application Security Testing (DAST), we utilize Invicti and Qualys Web Application Scanner (WAS).
    - For Software Composition Analysis (SCA) or third-party dependency analysis, we utilize OWASP Dependency Check, OWASP Dependency Track, FOSSA, JFrog Xray, and Trivy (specifically for container images).
    - Furthermore, we use OWASP Defect Dojo as our vulnerability management system.
    - We ensure that products are not released with vulnerabilities impacting our products.
- We **continuously scan third-party dependencies** for security vulnerabilities related to our supported products.
- Vulnerabilities that are discovered will be assessed for their impact. If any true-positive vulnerabilities are identified, immediate actions will be taken, such as implementing fixes and patches according to their severity, in line with our Vulnerability Management Process.

.

Product vulnerability and patch management

- WSO2 products are supported for three years upon a major release. WSO2 provides updates and patches for bugs and security issues during this period. Please refer to the support matrix for detailed information on supported products.
- Any vulnerability reported against WSO2 products would undergo the Security Vulnerability Management Process. Reported vulnerabilities will be assessed according to the CVSS scheme and fixed according to the given resolution timeframes.
- WSO2 has established a Security Reward and Acknowledgement Program where security researchers can analyze the security state of WSO2 products and report any identified security issues or vulnerabilities.

- WSO2 would first release patches to WSO2 customers via U2 (Update tool). After one month, when customers receive patches/updates, WSO2 publishes a security advisory on the Security Advisory page.
- In some instances, particular reported vulnerabilities would not apply to WSO2 products, and WSO2 may decide not to patch such. Those vulnerabilities would be listed on the CVE Justifications page.

WSO2 infrastructure security

- WSO2 Infrastructure is compliant with ISO 27001:2013.
- All workstations and servers are protected with an antivirus solution and regularly monitored as per ISO 27001:2013
- All workstations and servers are encrypted at rest.
- All workstations and servers are to install software that is approved and authorized.
- A central MDM solution manages all workstations and servers. A regular patch management process is in place as per ISO 27001:2013
- Conduct independent third-party audits annually, which are separated from annual ISO audits.
- Regular Internal and External VAPTs are conducted on WSO2 systems and network devices.
- All infrastructure-related incident responses are handled according to ISO 27001:2013.

Security guidelines for production deployment of WSO2 products

- WSO2 has published secure guidelines for production deployment. This guideline recommends configurations to secure all the production environment's all layers (OS, Network, and Application).
- Customers should adhere to the above guidelines to be secure and compliant when setting up products for production usage.
- Any product-related queries can be raised at the WSO2 support channels.

Security commitments of WSO2

- Adhere to the WSO2 Secure Engineering Guideline and WSO2 Secure Development processes when engineering WSO2 products.
- To ensure that product vulnerabilities are patched in compliance with the Support SLA.
- Upon request, provide customers with scan reports of static scanning, dynamic scanning, and software composition analysis reports to assist with customer compliance programs.
- WSO2 monitors for security issues related to 3rd party dependencies daily for the latest product release. All supported products will be patched per the WSO2 Security Vulnerability Management Process if a true positive vulnerability is identified.
- In case of a security incident or privacy breach impacting customers, WSO2 will reach out to customers within 72 hours of becoming aware of the relevant incident or breach.

- In case of a security incident, publically document the details on the Security Incident Clarification page.
- WSO2 would work proactively with customers to remediate security incidents and provide detailed information/reporting regarding security incidents impacting customers.

WSO2's Responsibilities

- WSO2 shall make "**Customer Security Announcements**" regarding product vulnerabilities and remediations via its support system with clear instructions on how to apply the same.
- WSO2 will share the following reports subject to appropriate confidentiality undertakings with customers.
    - Annual Independent party (External) VAPT reports of WSO2 Infrastructure.
    - Annual Independent party (External) audit reports of WSO2 Infrastructure.
    - ISO 27001:2013 Certificate and Audit Reports
    - WSO2 product-related security scan reports.
    - Provide customers with detailed root cause analysis and incident reports on security issues.

Customer's Responsibilities

- The customer must adhere to the security guidelines for production deployment when setting up the environment to ensure that products are set up securely.
- The customer must proactively monitor Customer Security Announcements made by WSO2 and **apply relevant remediation** after conducting testing on lower environments **within 30 calendar days after the Customer Security Announcements**.
    - It is recommended to prevent the exploitation of unpatched deployments after public disclosure. Public Announcements will be made after a minimum buffer of 30 calendar days from the Security Announcement, enabling customers to protect their deployments before public disclosure of the issue.
- The customer must adhere to the WSO2 Support Matrix and work toward upgrading/migrating to supported versions.
- If a customer is using WSO2 docker images, the customer must ensure that the customer is using the latest docker image from WSO2 Private Docker Registry.
- The customer should inform WSO2 about any vulnerabilities or security issues identified within WSO2 products.
- The customer must ensure that sensitive data has been appropriately sanitized before sharing data, logs, configurations, and dumps with WSO2 support teams.

- If a user with access to the WSO2 support portal no longer requires such access, inform WSO2 regarding the same immediately and get access revoked.
- The customer must proactively nominate users who should have access to the WSO2 support portal and Customer Security Announcements.
- The customer must denote the security point of contact(s) so that “Customer Security Announcements” would reach them promptly. WSO2 recommends having these notifications sent out to the customer's security team or security leadership, who would proactively work towards mitigating the risks.

Exclusions

WSO2 shall not be responsible for any security/breaches in respect of the following:

- If the customer gets compromised due to not monitoring the Customer Security Announcements proactively, remediation actions must be taken to safeguard deployment following such announcements.
- If the customer gets compromised due to not adhering to the security guidelines for production deployment.
- The customer gets compromised due to not migrating to supported product versions listed under the WSO2 Support Matrix.
- Customizations or extensions developed or integrated into WSO2 products by the customer.

Revision History

Release Date	Version	Summary of the Changes
2022-04-29	1.0.0	Initial version
2023-03-21	2.0.0	Fixed broken links and amended process updates
2024-12-26	3.0.0	Fixed broken links and amended process updates