SECURITY POLICIES

ManageEngine ITOM Products

www.manageengine.com/itom

Table of Contents

I. Organization security

ManageEngine, the Enterprise IT Management Software division of Zoho Corp., has a dedicated Information Security Management System (ISMS) in place which takes into account our security objectives, and the risks and mitigation concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

A. Employee background checks

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

B. Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

C. Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defence systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

D. Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties. Zoho has earned the following certifications for Applications, Systems, People, Technology, and Processes:

IS 642819

ISO/IEC 27001

- ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

PM 732705

ISO/IEC 27701

- ISO/IEC 27701 is an extension to the ISO/IEC 27001 and ISO/IEC 27002 standards for privacy management within the context of the organization. The certification standard is designed to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). This standard enables organizations to demonstrate compliance with the various privacy regulations around the world that are applicable to them.

- Zoho is SOC 2 Type II compliant. SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the AICPA's Trust Services Principles criteria.

- **Signal spam** reports help in providing FBL data, primarily technical information for identification of spammers and marketing abuse, from major ISPs like Orange.fr, SFR.fr, and so on. It has many spam reporting plug-ins for third-party browsers and email clients, focused at the French communities worldwide. It's important for both Zoho corporation and our customers to know all the recipients who mark or report the emails they receive as 'spam', so that we can remove them from the lists. Hence, this certification protects our network reputation in the French region.

The certifications mentioned above are applicable to all ManageEngine ITOM products. For more details, check out our compliance portfolio.

E. Endpoint security

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

II. Application security

A. Secure by Design

We adhere to the secure coding guidelines of the Software Development Life Cycle (SDLC) and these guidelines are shared to all developers. As the next step, we screen the code changes to look for potential security issues by first, manually reviewing it, and second, using our code analyzer, and vulnerability scanner tools. This entire process is carried out before the release of any new feature. If any issue is found, they are immediately checked and fixed. Furthermore, a robust security framework, that is based on the OWASP standards, is implemented in the application layer. This framework provides means to mitigate threats such as SQL Injection, Cross-Site Scripting, and Application Layer DoS attacks. To top it all, we conduct regular sessions to educate developers about secure coding practices.

B. Identity and Access control

- **Integration with identity stores:**

ManageEngine ITOM products readily integrate with external identity stores like Microsoft Active Directory and RADIUS servers. Users can be imported from identity stores and the respective authentication mechanism can be leveraged. Users will be uniquely identified through their respective accounts in the identity store.

- **Unique accounts and strong local authentication:**

ManageEngine ITOM products come with a local authentication mechanism in which unique accounts are created for users. Users will be able to access the application with their credentials. The credentials are one-way hashed using bcrypt, and are stored securely in the database located in the customer setup.

C. Encryption

- **At rest:**

Sensitive data, such as passwords, auth-tokens and the like, that are stored in the database are encrypted using 256-bit Advanced Encryption Standard (AES). For every customer, a unique installation key is generated and used for encryption.

- **Database Protection**

By default, the bundled PostgreSQL database in OpManager is only accessible by providing instance-specific credentials and is limited to local host access.

D. Protection against CSRF

A Cross-Site Request Forgery (CSRF) attack occurs when a malicious website/ blog or a program causes the web browser used to perform actions that are not authenticated by the user. This poses a serious threat to a user's critical data. Generally, the lack of a proper authentication mechanism makes a user's web browser vulnerable to CSRF attacks.

OpManager provides protection against CSRF attacks. This ensures that a customer's critical information and credentials stay protected and are not prone to external threats or exploitation.

E. Patch integrity verification

In OpManager, the integrity verification for patches applied will done during the upgrade process. To enhance security, all unknown patches applied to the installed application will be restricted.

III. Operational security

A. Customer data security:

The customer data resides only in their environment, as the product is an on-premise solution.

****Note:** In case any customer requires help in resolving any issue, we may require the customer's logs. The customer uploads the logs through a secure portal owned by us, that can be accessed only by authorized personnel, and grants us permission to access them. The logs will be deleted automatically after five days from the time of upload.

B. Vulnerability mitigation and patch management:

We have a dedicated vulnerability process that actively scans for security threats or vulnerabilities using a combination of certified third-party scanning tools, and in-house tools. Subsequently, automated and manual testing is performed. Furthermore, the security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to identify security incidents that might affect the company. Once we identify a vulnerability that requires remediation, it is logged, prioritized according to severity, and is assigned an owner. We further identify the associated risks and mitigate them by patching the vulnerable systems. After assessing the severity of the vulnerability based on the impact analysis, we commit to resolve the issue within our defined SLA. Depending upon the severity, we send security advisories to all our customers describing the vulnerability, the patch and the steps to be taken by the customer.

C. Business continuity:

- We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as, infrastructure management and technical support.

- We have a well planned business continuity and disaster recovery plan in

place to assist us in the event of natural calamities, man-made disasters, etc. The plan encompasses all our internal operations that ensure continued services for our customers. We have three recovery teams namely, the Emergency Management Team (EMT), the Disaster Recovery Team (DRT), and the IT Technical Services (IT) team, in place for better coordination and support among various teams.

D. Responsible Disclosure

A vulnerability reporting program in "Bug Bounty", to reach the community of researchers, is in place, which recognizes and rewards the work of security researchers. We are committed to working with the community to verify, reproduce, respond, legitimate, and implement appropriate solutions for the reported vulnerabilities. If you happen to find any, please submit the issues at https://bugbounty.zoho.com/

If you want to report vulnerabilities to us directly, drop a mail to security@zohocorp.com

E. Customer controls for security

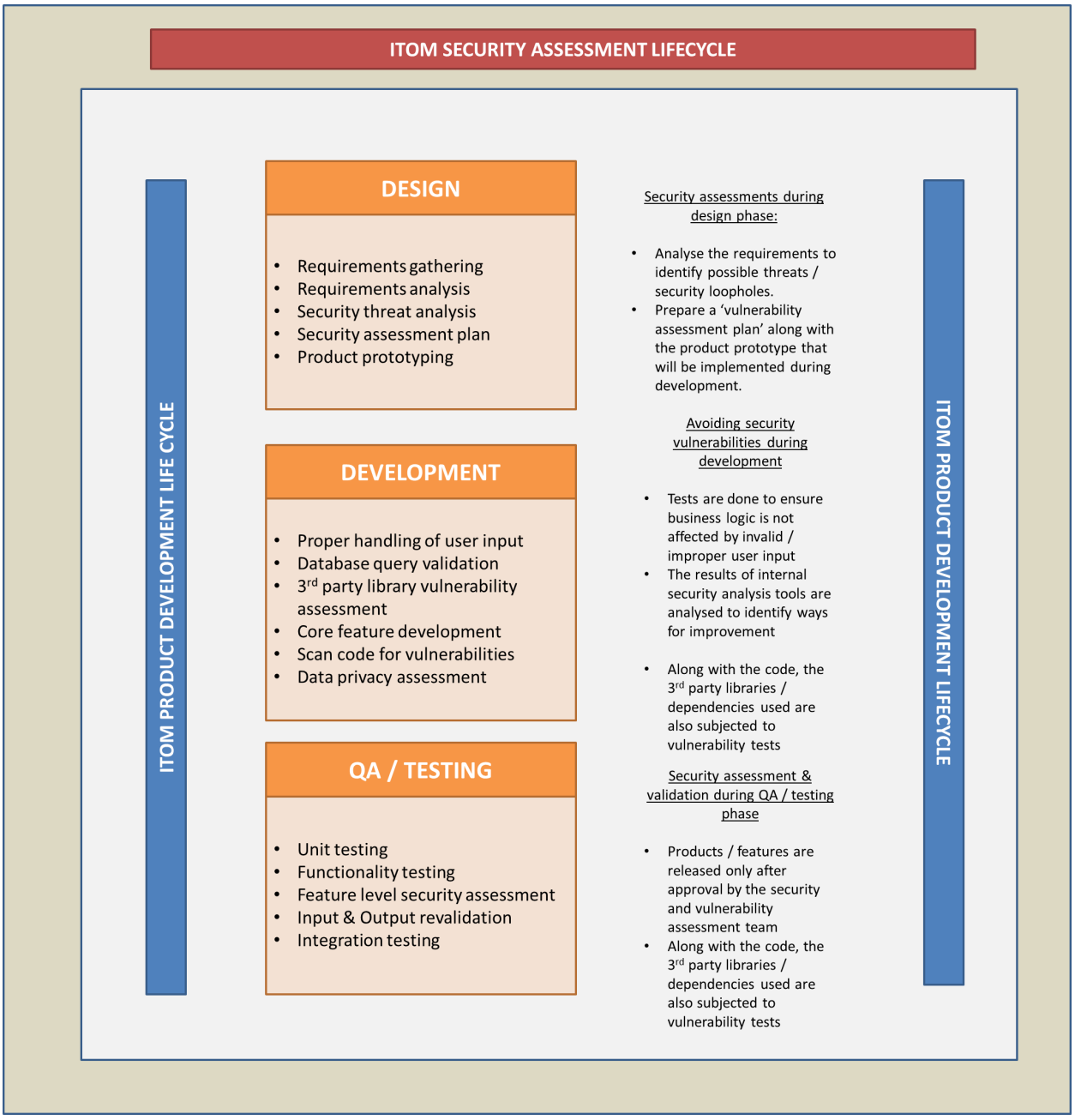
So far, we have discussed what we do to enhance security on various fronts to our customers. Here are the things that you as a customer can do to ensure security from your end:

1. Make sure that the application is installed with required privileges.
2. To ensure secure connections, enable HTTPS mode of communication and use only trusted third party certificates.
3. Change the default admin password as soon as the set up is complete.
4. Use complex passwords and change the user passwords periodically.
5. Enable Two Factor Authentication (TFA) as an additional security layer to prevent unauthorized access.
6. Monitor the users who have access to the application under the User Management section and verify them periodically.
7. If 'Network Shared Folders' are configured in the product, then make sure that the folders are secured.

8. Keep your applications up-to-date.
9. Review the audit logs periodically.
10. Periodically backup application data and the database.
11. Enable failover/hot standby for high availability which helps in 24*7 monitoring of your networks.

Note: It is advised in the best interest of customers to read the security best practices enumerated in our site and exercise them while using the product.

IV. Security assessment lifecycle



The security assessment life cycle is a part of the complete SDLC (Software Development Life Cycle) process through which all the ITOM applications are subjected to before they are released into the market. The assessment of security and vulnerability is done in every part of the application development process (Design, Development & QA).

A few prominent pre-checks that are done in the security assessment lifecycle to ensure that the application does not become victim to any security issues include :

- All third party dependencies in the code are run through vulnerability check tools before they are inducted into the code.
- All user input is subjected to proper validation.
- Access privilege system is firmly adopted in all phases in the applications.
- Every module in the code is OWASP compliant.
- The release of every feature in the product is subjected to the approval of the security and vulnerability assessment team and also the approval of the module owner who handles to ensuring that the product is well secured from any vulnerabilities.
- The reports from the internal security tools are periodically analyzed to identify possible improvements that can be made to the security assessment lifecycle.

The ITOM security assessment lifecycle focuses on the following important security vulnerabilities:

1. XSS Vulnerability
2. SQL Injection
3. Path Traversal
4. Local File Inclusions
5. Remote code execution
6. XML Injection
7. Other common vulnerabilities such as deserialization of untrusted data, untrusted dynamic class loading, weak algorithms, zip bomb, etc.,

V. FAQs on security practices

Q. How do we ensure security in the product development life cycle?

ManageEngine ITOM products are developed only by our employees who are qualified engineers. We follow industry-best software development practices to ensure the integrity of the code and the product. Every line of code developed goes through two levels of security check. First, it is reviewed by the Leads\Manager for both performance and security. Second, we have dedicated security teams for auditing the build that is taken for release to ensure that there are no open doors for attacks/hacks. If either of them are not satisfied with the security measures, then that particular build will not be released.

Q. How are third party components introduced in the product?

The third party components (JAR, .js, etc.,) are extensively checked for CVE or security issues by the security team. Any third party component that is used in the development of the product is integrated only after the approval of the security teams.

Q. How do we ensure security in the release process?

Once the build is ready for release, it is subjected to multiple vulnerability tests. Only the builds that pass the tests are taken for release. This helps us provide highly secure software products. We ensure that the changes made after the previous build alone are integrated in the upcoming release.

Q. Given the current situation, how does ManageEngine ensure the integrity of the builds available for download in its domain?

Every ITOM product (.exe/.bin) available for download in the ManageEngine domain is Checksum verified to ensure its integrity. Again, the builds were downloaded and manually checked for the presence of any malicious code, for enhanced security. The builds available on our website are found to be intact.

For any queries, kindly drop a mail to opmanager-support@manageengine.com