ATOSS

R&D Security Process for ATOSS Staff Efficiency Suite and ATOSS Time Control | External

Version: 2.00
Last Edit Date: 18.03.2020

Disclaimer: The document focusses on the ATOSS main products ATOSS Staff Efficiency Suite and ATOSS Time Control. It does not include security aspects related to

- Crewmeister
- the infrastructure of the ATOSS Cloud Solution
- the ATOSS internal IT infrastructure

Content

0. Preface

Security is our value

ATOSS takes the security of its products very seriously, with a comprehensive secure software development life-cycle process and clear quality and security standards for software development. There is a dedicated Security Response Process in place as the most visible evidence of our commitment. The ATOSS R&D team is responsible for investigating all reported security vulnerabilities, working closely with the reporters of vulnerabilities to provide patches. ATOSS informs the customers about the patches and their importance. Since the integrity and security of business operations is crucial for businesses in all industries, ATOSS as a provider of business software is absolutely committed to maintaining the highest possible level of security within its products.
ATOSS encourages the responsible disclosure of security vulnerabilities. If you have detected a vulnerability in one of our software products – either in the latest or in a former product version – please inform us about the issue and send an email to security@atoss.com.

Give ATOSS sufficient time to develop suitable fixes

- Fixing security vulnerabilities can be a long and arduous process as we work to develop a patch, ensure its compatibility with all relevant software versions, run comprehensive tests to ensure that the fixes run well and do not have any side-effects, and provide it to our customers.
- As a vendor of business software we provide security fixes not only for the latest version, but also for many older versions of our software products. This means that we need to develop and thoroughly test feasible patches for a broad range of product versions, which can take time.

Do not publicize vulnerabilities until ATOSS customers have had time to deploy fixes

The deployment of patches for ATOSS products is usually more complicated than a software upgrade on a consumer PC. Depending on the nature of the vulnerability, the deployment of patches or updates in some cases requires configuration or deployment tasks with regard to customer internal restriction or processes. Some of our customers follow for example regular patching cycles. Considering these circumstances, we ask all security researchers to give ATOSS customers sufficient time to implement patches in their systems. As a rule of thumb, we suggest respecting an implementation time at customer site of three months once the patch is released by ATOSS. Considering our customer interests, we ask all security researchers to not disseminate any kind of information or tools that would help to exploit the vulnerability during that time.

Please also inform the R&D team about all your upcoming public advisories and external presentations with ATOSS product security content via e-mail to security@atoss.com. including the intended content at least 3 weeks in advance.

1. Main standards and recommendations

ATOSS uses relevant sources to collect the information regarding security issues and measures to protect applications. Besides information that is published by third party product companies that are used by ATOSS (such as ORACLE, etc.) we mainly focus on the following internationally agreed sources:

- BSI Bundesamt für Sicherheit in der IT: IT-Grundschutz, Baustein 'APP Anwendungen', APP 3.1 Webanwendungen'
- OWASP Open Web Application Security Project: Open Web Application Security Project

Their publications are analyzed continuously and thoroughly. Aspects that are applicable to the ATOSS products are examined in detail and followed by measures during the R&D internal product development cycle. Details see below.

2. Overview About The Security Process

The process follows the Standard Risk Management process cycle aspects:

Identification: The ATOSS internal Security Process has three components that complement each other:

- Together with an external partner we address the main security issue: creativity and "hacker-"related knowledge. On a regular basis - depending on changes in the technology of our application or findings of our partner we define testing cycles during the QA-Phase of the determined release. Normally these external tests are done on a yearly basis. If necessary they are done more often (*External Security Audit*).

- ATOSS regularly checks our security internally during the dedicated QA-Phase within our 4-month software release cycle by a careful internal security (regression) test based on Industry Standard tools and on manual testing of new security related features (*Internal Security Test*).
- ATOSS constructs security by implementing secure software with regard to the upper mentioned sources (*Construct Security*).

Analyze and Rating: All findings are documented and rated using the *Security Issue Priority Scheme* (see below).

Measures and Control: Depending on the rating all findings are treated effectively via the *Security Response Process* which consists of the following subprocesses:

- Urgent findings are treated via the *Important Update Process*.
- Relevant findings without the highest urgency which nevertheless need to be treated in a release that is already in development via the *Support Feature Process.*
- All findings that do take more effort, contain relevant risk for existing functionality or are not critical are addressed via the *Regular Release Process.*

Documentation: All issues and related results are documented in a ***Security Report*** which is updated with each release but not delivered explicitely to customers following the BSI Information Policy.

3. Identification of Security Issues

External Security Audit

The goal of this audit is to validate the ATOSS products' security level via independent checks against a "State-of-the-Art" level ('external penetration test'). In case there are findings they are treated according to the *Security Response Process*. This audit takes place in coordination with our external partner as often as the partner - together with the R&D department leads - sees the necessity due to technical changes in the interior or outer world. This is done in balance between expected changes and test invest on both sides. The test is normally coordinated with the internal release cycle in order to allow optimal response times. This means currently the tests take place during the QA-phase of a new release. All findings are rated following the *Security Issue Priority Scheme*.

The audit delivers a test result which is integrated in the *Security Report* which is updated for every release (see below).

Internal Security Tests

The goal of this test is to validate the ATOSS products' security level within every new release. We are heading for two directions:

1. Ensure the existing quality by regression tests. Therefore we use Industry Standard tools like BURP. In case there are findings they are treated according to the *Security Response Process*. This process takes place during the QA phase of every release
2. Test new security findings: All findings that are implemented during a release are manually checked and tested by our QA experts. If there are findings they are rated again following the *Security Issue Priority Scheme*.

The test also delivers a test result which is integrated into the *Security Report* which is updated for every release (see below).

Analyze and Construct Security

The goal of this measure is to construct new features in a secure way. Therefore all team members are made sensitive on designing new features to mark all features that may have security impact. The R&D team reviews this and collects all potentially security relevant issues until the beginning of the planning phase of a release. This collection is fed from the following sources:

- Reported security issues from customers or partners
- External security tests ordered by ATOSS
- Relevant newsletters (US Homeland Security, Heise, etc.)
- Public news
- Audit results and penetration test findings performed by customers or partners
- Internally discovered issues
- Automatic tests (CrashtestSecurity, currently on TAI)
- These major information sources are checked regarding the latest security information of the
  JAVA and Tomcat environment:
  - https://www.oracle.com/security-alerts/
  - https://www.us-cert.gov/ncas/alerts
  - https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-23642/Oracle-Openjdk.html
  - https://tomcat.apache.org/security-9.html
  - Relevant vulnerabilities will result in an issue to update to a newer version
- All **third party libraries** used on client and server side are scanned each release using a standard tool (https://owasp.org/www-project-dependency-check/) based on the maven dependencies. The results are analysed and libraries to update or replaced are identified.
- Sonar Qube static code analysis report

All incoming security issues are analyzed based on the *Security Issue Priority Scheme.* For issues that are planned for a release the technology department gives a clear design proposal, carefully reviews the final design and the technical implementation to ensure a secure and high-Quality implementation. All other issues are collected in a security backlog that is reused for the planning of further releases.

4. Analyze and Rating along the Security Issue Priority Scheme

Priority	**CVSS Range (if applicable)**	**Classification**	**Security Response (Sub) Process**	**Customer Information Process***
Low	0 - 3.9	Hinder the user experience / quality of service No risk of data leaking or data loss.	Consider fixing in one of the next releases (*Regular Development Process*)	Publish in Release Notes if applicable
Medium	4 - 6.9	e.g. Risk of read access to unauthorized data.	Fix in an upcoming release (*Support Feature Process*)	Publish in Release Notes if applicable
High	7 - 8.9	e.g. Risk of write access to unauthorized data	Fix immediately (*Important Update Process*)	Identify affected customers and recommend an update (Important Update process)
Critical	9 - 10	e.g. Risk of read / write access beyond the ATOSS system boundaries.	Fix immediately (*Important Update Process*)	Identify affected customers and strongly recommend an update (Important Update process)

The effective prioritization will consider the risks and the probability that the vulnerability can actually be exploited in the ATOSS Staff Efficiency Suite or ATOSS Time Control.

* The customers are informed, as soon as a solution for the security issue exists.

5. Measures along the Security Response Process

Important Update Process

This solution is identically used for "Critical" and "High" functional issues. All team members in all relevant departments are aware of this process. The handling of the security issue starts at the working day where it was detected and classified accordingly to ensure the fastest possible solution. It contains a detailed description of the effective internal treatment, the build of update- or patch versions, a communication strategy towards affected customers and an offer for support in case the customers needs this. The process is carefully documented and tracked until all affected customers at least confirmed the knowledge about the issue and its fix.

Support Feature Process

This process is used for security issues of the priority 'Medium'. It is integrated in the release and takes care about security issues of minor criticality that need to be treated not only in the next release but also in releases which are currently in development. This means these cases are not postponed to a later release but are critical enough to change the planning of the currently release developed. You may also name this feature a "change" to the current release.

Regular Development Process

This is used for security issues of the priority 'Low'. This means, the feature needs not to be delivered in short time. Therefore the implementation is planned in a standard way. It is added to the backlog of features that are considered due to the "Construct Security" Analysis of the next release (see above). The planning and fixing of these security issues follows the standard 4-month release cycle. All issues planned in a release are collected and documented in a table with the following structure. All features that are plannend and delivered in a release are documented in the same format which is part of the ***Security Report***.

Date	External Source	Decision: No Risk / not relevant	Risk	Planned for Release
	<Source 1>	<Reason>	<Link to Jira/Bugzilla-issue. Set the Jira flags 'Security issue' and 'Relevant for security'>	Version

6. Control and Escalation

All upper mentioned processes do have a clear responsible role which controls the fulfillment of the measure to fix the security issue. For important updates the Head of Product Development is responsible, for the Support Feature Process and the Regular Development Process both the Release Manager is responsible. In case a measure does not have the intended effect there is an escalation report to the Management Board for further measures and decisions. This assures the most effective measures even in case of problems. Further on as a standard process in R&D a feedback and review process is established which checks for possibilities of improvement. This means this security process is reviewed also on a release-based circle.

7. Monitoring: The Security report

There is an internal security report for every release for the ATOSS Staff Efficiency Suite and the ATOSS Time Control which collects the upper mentioned results of the analysis, the rating, the measures and the results. Concretely it contains the following sections:

1. Features implemented by the regular development process as a table with description and test results
2. Findings of internal security regression test and measures
3. Findings of external security regression tests and measures
4. Diverse aspects - like documentation of external findings and resulting important update results

ATOSS Software AG | Rosenheimer Straße 141 h | 81671 München | Deutschland | security@atoss.com | www.atoss.com