ATOSS R&D Security Process

for software development

v. 07-2022

This document is for information purposes only. It summarizes information about the current R&D Security Process for software development of ATOSS Software AG and its affiliated companies (hereinafter "ATOSS"), which may be amended and updated from time to time. The current version of this document is available for download from our website under "Security". The statements in this document do not constitute any binding promises or representations by ATOSS, subcontractors or licensors.

Notwithstanding the foregoing, ATOSS intends to provide customers with more in-depth background information regarding security in ATOSS products.

This document focuses on the ATOSS products, ATOSS Staff Efficiency Suite, ATOSS Startup Edition and ATOSS Time Control.

It does not contain any security aspects regarding

- Crewmeister products
- the ATOSS Cloud Services infrastructure
- the ATOSS internal IT-infrastructure

Table of content

A. Foreword

Security is very important to us

As the integrity and security of business operations are essential for all companies in all industries, ATOSS as a service provider of HR Workforce Management Software strives to maintaining the highest possible level of security in its products.

The most visible proof of our commitment is an established dedicated process for responding to security issues. The ATOSS R&D team is responsible for investigating all security vulnerabilities that have become known or have been reported to ATOSS. The ATOSS R&D team initiates the defined processes for patch management and coordinates and supports the responsible disclosure of security vulnerabilities to affected customers through to the provision of security updates.

In order to inform our customers transparently and promptly about the most important developments regarding known security issues, the ATOSS R&D team updates and publishes new security notices as well as upcoming security updates under the following link:
Security News | ATOSS AG

Therefore, please check our website for all published security advisories regarding ATOSS products.

Report security issues to us

If you have noticed a security vulnerability in one of our ATOSS products – either in the latest product version or an earlier one – please notify us in an e-mail to security@atoss.com.

Allow ATOSS sufficient time to develop suitable security updates

Resolving security vulnerabilities can be a lengthy and complicated process. We develop a security update, make sure that it is compatible with relevant software versions, carry out extensive tests to ensure that it runs as possible without side effects, and make it available to our customers.

Do not publish any security vulnerabilities or associated information until ATOSS customers have had time to roll out their security updates.

Depending on the nature of the vulnerability, deploying security updates may in some cases require configuration or deployment tasks that consider internal customer constraints or processes. For example, some of our On Premises customers follow regular patch cycles and cannot act immediately.

In due consideration of these circumstances, we request you on behalf of these ATOSS customers to give them appropriate time to install security updates in their systems. As a rule of thumb, we suggest allowing customers an installation period of three (3) months as soon as the security update has been released by ATOSS. In due consideration of our customers' interests, we request you not to circulate any information or tools that could contribute to exploiting the security vulnerability during this time.

In addition, please inform the ATOSS R&D team at least three weeks in advance of all security information that you would like to publish, or upcoming external presentations with security content from ATOSS products, in an e-mail to security@atoss.com that includes the intended content.

B. Main standards and recommendations

ATOSS takes the security of its products very seriously.

To this end, ATOSS has a comprehensive process for a secure software development lifecycle as well as clear quality and security standards for software development.

The ATOSS R&D team therefore uses relevant sources to collect information about security issues and measures. In addition to information published by third party providers whose products ATOSS uses (e.g. ORACLE etc.), the ATOSS R&D team mainly concentrates on the following internationally agreed sources:

Federal Office for Information Security ("BSI"):	IT-Grundschutz, Baustein 'APP Anwendungen', APP 3.1 Webanwendungen und Webservices'
OWASP Open Web Application Security Project:	Open Web Application Security Project

These publications are routinely analyzed. Appropriate measures are derived from security aspects affecting ATOSS products in the internal R&D product development cycle.

C. Overview of the R&D security process

The process for secure software development life cycle is structured as follows:

1. Step - Identification of security problems

The identification phase contains three sub-aspects that complement each other:

- *Build security* - ATOSS builds security by implementing secure software in accordance with the guidelines from the above-mentioned sources.
- *Internal security audits* - ATOSS checks its security regularly during the QA phase within a four-month software release cycle, by means of careful internal security tests ("regression tests"). On the one hand, these are based both on standard tools and static code analyses of the entire code base. On the other hand, they are carried out internally, as well as commissioned to an external service provider within the context of (re)certification for SAP integration certification ("Premium Certification as an SAP Endorsed App"). In both cases, we use the product Veracode, the current market leader in this area. Finally, new features are checked for their security by means of manual tests. All of these components make up the Internal security test.
- *External security audits* - In cooperation with external security companies, we address two (2) further important security threats: creativity and "hacker"-related knowledge. On a regular basis – although also dependent on the number and relevance of the changes in the technology used in our ATOSS products or the security vulnerabilities that external security companies have discovered previously – we define appropriate test cycles during the QA phase of the respective release. External security tests take place regularly, but at least once a year.

2. Step - Analysis and assessment

All security issues findings are documented and assessed using the security issues priority scheme (defined below).

3. Step - Measures and monitoring

In accordance with the evaluation, all security vulnerabilities found are resolved within the security response process.

This consists of the following sub processes:

- The Process for important updates handles serious vulnerabilities.
- The Process for support features handles relevant vulnerabilities that do not have the highest priority, but must still be dealt with promptly, i.e. in a release that is already in development.
- The Process for regular development handles all remaining vulnerabilities that do not carry any relevant risks to existing functionality and require more effort to resolve.

4. Step - Documentation

All resolved vulnerabilities are documented in a security report for every release. However, in accordance with the information policy recommended by the BSI, this report is not explicitly delivered to customers.

In detail:

1. Step - Identification of security issues

Analyzing and build security

The objective of this measure is to build new features securely. When designing new features, all team members are therefore sensitized to highlighting features that could affect security. The R&D team checks these and collects all issues potentially relevant to security up until the beginning of the planning phase of a release.

This collection comes from the following sources:

- Security issues reported by customers or partners
- External security tests commissioned by ATOSS
- Relevant newsletters (US Homeland Security, Heise etc.)
- The news
- Audit results and penetration tests of customers or partners
- Issues discovered internally
- Automatic tests (Crashtest Security, currently on TAI)
- These key sources of information are checked for the latest security information regarding 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 security vulnerabilities result in the need to upgrade to a newer version. All third-party libraries used on client and server are scanned in each release using a standard tool based on the Maven dependencies. The results are analysed and libraries to be updated or replaced are identified.

  - https://owasp.org/www-project-dependency-check/
  - Sonar Qube static code analysis report

All incoming security issues are analysed, based on the security issue priority scheme. In the case of issues scheduled for a release, the ATOSS R&D team suggests a "secure" design and checks the final technical design and the technical implementation carefully in order to ensure a secure and high-quality implementation. Any remaining vulnerabilities of low criticality that cannot be resolved in the current release, are collected in a security backlog that will be further processed when further releases are scheduled.

Internal security audits

The objective of internal security audits is to validate the security level of ATOSS products within every new release.

We follow several directions:

- Safeguard the existing quality by means of regression tests. We therefore use tools from our branch of industry, such as BURP. Any findings are handled in accordance with the security response process. This process takes place during the QA phase of each release.
- The existing code undergoes a static code analysis, based on Veracode, at regular intervals.
- Check resolved security vulnerabilities: all vulnerabilities resolved during a release are checked and tested by our QA experts manually, in addition to using the tools described. In case new vulnerabilities are found, they are re-evaluated against the security issue priority scheme. The vulnerabilities found and resolved in this test are documented in the security report.

External security audits

The objective of external security audit is to validate the security level of ATOSS products against a "state-of-the-art" level by means of independent checks. If anything is found, these security vulnerabilities are dealt with in accordance with the security response process. This audit takes place in collaboration with our external partner, as often as the partner – in cooperation with the ATOSS R&D team leads – considers it necessary owing to technical changes within or outside of the company. Expected changes and investments in tests are weighed against each other. The audit is normally coordinated with the internal release cycle in order to ensure optimum response times. This means that the tests currently take place during the QA phase of a new release. All findings are evaluated on the basis of the security issue priority scheme. In addition, the entire code base undergoes a static code analysis with a further partner at regular intervals – typically once per release – in order to check for security vulnerabilities for recertification as part of the SAP integration certification ("Premium Certification as an SAP Endorsed App").

The vulnerabilities found and resolved in the audit are also documented in the security report.

2. Step - Analysis and assessment

Customers will be informed as soon as there is a solution for the security issues exists.

The analysis and evaluation are done based on the priority scheme for security issues

Priority	**CVSS range (if applicable)**	**Classification**	**Security response (sub)process**	**Customer information process***
Low	0–3.9	Impedes the user experience/service quality No risk of data leakage or data loss	Consider resolving in one of the next releases (*Process for Regular Development*)	Publish in Release Notes, if applicable
Medium	4–6.9	E.g. risk of read access to unauthorised data	Resolve in the next release (*Process for Support Features*)	Publish in Release Notes, if applicable
High	7–8.9	E.g. risk of write access to unauthorised data	Resolve immediately (*Process for Important Updates)*	Identify customers affected and recommend update
Critical	9–10	E.g. risk of read/write access beyond the boundaries of the ATOSS systems	Resolve immediately (*Process for Important Updates)*	Identify customers affected and recommend update

The effective prioritisation considers the risks and probability that the security vulnerability can actually be exploited in den ATOSS products.

3. Step - Measures and controls

Process for regular software development

This process is used for security issues with “low” priority. This prioritisation does not require the issue to be resolved promptly. For this reason, these issues are scheduled to be resolved within regular release development. They are added to the backlog of features that will be taken into account for the “Build security” analysis of the next release (see above). These security issues are scheduled to be resolved as part of the four-month standard release cycle.

Process for support features

This process is used for security issues with “medium” priority. It is integrated in the release. The security issues that must also be dealt with in the release currently still in development are handled by means of this process.

Process for important updates

This process is identical for security issues rated as “critical” and “high”.

All team members in all relevant business departments are aware of this process. The security issue starts to be dealt with on the working day on which it was detected and appropriately classified, to guarantee the fastest possible solution. The solution to be found will contain a detailed description of how the issue was effectively handled internally, the creation of build or patch versions, a communication strategy for the customers affected and, if necessary, a support offer, if the customer so requires. The process for resolving the security issue is carefully documented and monitored until all customers affected have at least been informed of the issue and how it has been resolved.

Control and escalation

Responsible roles for monitoring the measures to resolve the security issue are defined for all the processes mentioned above. In the case of the process for important updates, the product development lead is responsible; in the case of the process for support features and the process for regular software development, the release manager is responsible. If a measure does not have the desired effect, an escalation report is sent to the management board for further measures and decisions. At the ATOSS R&D team there is also a feedback and check process, within which possibilities for improvement are examined after every critical incident.

4. Step - Documentation

For every release, the ATOSS R&D team creates an internal security report that summarises the above-mentioned analysis results, assessment, measures and controls.

ATOSS.COM

ATOSS Software AG
Rosenheimer Str. 141 h
81671 Munich
Germany
T +49 89 4 27 71 0

ATOSS Software Ges.m.b.H.
Ungargasse 64-66/3/503
1030 Vienna
Austria
T +43 1 710 57 68 0

ATOSS Software AG
Luggwegstr. 9
8048 Zurich
Switzerland
T +41 44 501 53 00

ATOSS Software AG
Rue aux Laines 70 Wolstraat
1000 Brussels
Belgium
T +32 2 781 18 50

ATOSS Software AG
Newtonlaan 115
3584 BH Utrecht
Netherlands
T +31 30 210 60 28

ATOSS Software AG
Vasagatan 7
111 20 Stockholm
Sweden
T +46 84 650 26 82

For more information visit our website www.atoss.com or email us to internet@atoss.com