ATOSS R&D Sicherheitsprozess

für Softwareentwicklung

v. 07-2022

Dieses Dokument dient ausschließlich zu Informationszwecken. Es fasst Informationen über den aktuellen R&D Sicherheitsprozess für Softwareentwicklung der ATOSS Software AG und ihren verbundenen Unternehmen (nachfolgend "ATOSS") zusammen, der von Zeit zu Zeit geändert und aktualisiert werden kann. Die aktuelle Version dieses Dokuments steht auf unserer Website unter "Security" zum Download bereit. Die Ausführungen in diesem Dokument begründen keine verbindlichen Zusagen oder Zusicherungen von ATOSS, Unterauftragsverarbeitern oder Lizenzgebern.

Ungeachtet dessen möchte ATOSS den Kunden vertiefende Hintergrundinformationen über die Sicherheit in ATOSS Produkten vermitteln.

Dieses Dokument konzentriert sich auf die ATOSS Produkte, ATOSS Staff Efficiency Suite, ATOSS Startup Edition und ATOSS Time Control.

Es beinhaltet keine Sicherheitsaspekte im Hinblick auf

- Crewmeister Produkte
- die Infrastruktur der ATOSS Cloud Services
- die ATOSS interne IT-Infrastruktur

Inhaltsverzeichnis

A. Vorwort

Sicherheit ist uns wichtig

Da die Integrität und Sicherheit des Geschäftsbetriebs für alle Unternehmen in allen Branchen essenziell sind, setzt sich ATOSS als Anbieter von HR Workforce Management Software dafür ein, in seinen Produkten eine höchstmögliche Sicherheitsstufe aufrechtzuerhalten.

Der sichtbarste Beweis für unser Engagement ist ein etablierter dedizierter Prozess zur Reaktion auf Sicherheitsprobleme. Das ATOSS R&D-Team ist dafür verantwortlich, alle bekannt gewordenen oder an ATOSS gemeldeten Sicherheitslücken zu untersuchen. Das ATOSS R&D Team initiiert die definierten Prozesse zum Patch Management und koordiniert und unterstützt die verantwortungsbewusste Offenlegung von Sicherheitslücken gegenüber betroffenen Kunden bis hin zur Bereitstellung der Sicherheitsupdates.

Um unsere Kunden transparent und zeitnah über die wichtigsten Entwicklungen zu bekanntgewordenen Sicherheitsthemen zu informieren, aktualisiert und veröffentlicht das ATOSS R&D Team neue Sicherheitshinweise sowie anstehende Sicherheitsupdates unter dem folgenden Link:
Security News | ATOSS AG

Bitte informieren Sie sich daher auf unserer Website über alle veröffentlichten Sicherheitshinweise zu den ATOSS Produkten.

Melden Sie uns Sicherheitsprobleme

Wenn Ihnen in einem unserer ATOSS Produkte eine Sicherheitslücke aufgefallen ist – entweder in der neuesten oder in einer älteren Produktversion – informieren Sie uns bitte in einer E-Mail an security@atoss.com.

Geben Sie ATOSS genügend Zeit zur Entwicklung passender Sicherheitsupdates

Das Beheben von Sicherheitslücken kann langwierig und kompliziert sein. Wir entwickeln ein Sicherheitsupdate, stellen sicher, dass er mit den relevanten Softwareversionen kompatibel ist, führen umfassende Tests durch, damit die Korrekturen möglichst ohne Nebenwirkungen laufen, und stellen ihn unseren Kunden zur Verfügung.

Veröffentlichen Sie keine Sicherheitslücken oder damit im Zusammenhang stehende Informationen, bevor ATOSS Zeit hatte, ihre Sicherheitsupdates bereitzustellen.

Je nach Art der Sicherheitslücke sind für die Bereitstellung von Sicherheitsupdates in manchen Fällen Konfigurations- bzw. Bereitstellungsaufgaben unter Berücksichtigung kundeninterner Beschränkungen oder Prozesse erforderlich. Einige unserer On Premises Kunden folgen beispielsweise regelmäßigen Patchzyklen und können nicht sofort handeln.

Unter Berücksichtigung dieser Umstände bitten wir Sie im Namen dieser Kunden, diesen genügend Zeit dafür zu geben, Sicherheitsupdates in ihren Systemen einzuspielen. Als Faustregel schlagen wir vor, den Kunden eine Einspielzeit von drei (3) Monaten zuzugestehen, sobald das Sicherheitsupdate von ATOSS bereitgestellt wurde. Unter Berücksichtigung unserer Kundeninteressen bitten wir Sie, keine Informationen oder Tools in Umlauf zu bringen, die in dieser Zeit dazu beitragen könnten, die Sicherheitslücke auszunutzen.

Bitte informieren Sie außerdem das ATOSS R&D-Team mindestens drei Wochen im Voraus über alle Sicherheitshinweise, die Sie veröffentlichen möchten, oder anstehende externe Präsentationen mit Sicherheitsinhalt aus ATOSS Produkten in einer E-Mail an **security@atoss.com** einschließlich des voraussichtlichen Inhalts.

B. Hauptstandards und Empfehlungen

ATOSS nimmt die Sicherheit seiner Produkte sehr ernst.

Dazu verfügt ATOSS über einen umfassenden Prozess für einen sicheren Softwareentwicklungs-Lebenszyklus sowie klare Qualitäts- und Sicherheitsstandards für die Softwareentwicklung.

Das ATOSS R&D Team verwendet hierzu relevante Quellen zum Sammeln von Informationen bezüglich Sicherheitsproblemen und Maßnahmen. Neben den von Drittanbietern veröffentlichten Informationen, deren Komponenten in ATOSS Produkten verwendet werden (z. B. ORACLE etc.), konzentriert sich das ATOSS R&D Team insbesondere auf die Auswertung von folgenden international vereinbarten Quellen:

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

Diese Veröffentlichungen werden routinemäßig analysiert. Aus Sicherheitsaspekten, die die ATOSS Produkte betreffen, werden im R&D-internen Produktentwicklungszyklus entsprechende Maßnahmen abgeleitet.

C. Überblick über den R&D Sicherheitsprozess

Der Prozess für einen sicheren Softwareentwicklungs-Lebenszyklus gliedert sich wie folgt:

1. Schritt - Identifizierung von Sicherheitsproblemen

Die Identifizierung-Phase enthält drei Teilaspekte, die sich gegenseitig ergänzen:

- *Sicherheit konstruieren* - ATOSS konstruiert Sicherheit durch die Implementierung sicherer Software gemäß den Vorgaben aus den oben genannten Quellen.
- *Interne Sicherheitsaudits* - ATOSS prüft seine Sicherheit regelmäßig während der QA-Phase innerhalb eines viermonatigen Software Releasezyklus durch sorgfältige interne Sicherheitstests ("Regressionstests"). Diese basieren einerseits auf Standardtools. Andererseits werden statische Codeanalysen der gesamten Codebasis durchgeführt. Diese werden sowohl intern durchgeführt als auch über einen externen Dienstleister im Rahmen der (Re-) Zertifizierung für die **SAP Integration Certification („Premium Certification as an SAP Endorsed App“)** beauftragt. Hierfür verwenden wir in beiden Fällen das Produkt Veracode, den aktuellen Marktführer in diesem Bereich. Zuletzt werden mittels manueller Tests neue Features auf ihre Sicherheit überprüft.
- *Externe Sicherheitsaudits* - Zusammen mit externen Sicherheitsunternehmen gehen wir zwei (2) weitere wesentliche Sicherheitsgefährdungen an: Kreativität und auf "Hacker" bezogenes Wissen. Regelmäßig, allerdings auch abhängig von der Anzahl und Relevanz der Änderungen bei der verwendeten Technologie in unseren ATOSS Produkten oder den Sicherheitslücken, die externe Sicherheitsunternehmen gefunden haben, definieren wir während der QA-Phase des jeweiligen Releases entsprechende Testzyklen. Externe Sicherheitsaudits finden regelmäßig, mindestens jedoch einmal pro Jahr statt.

2. Schritt - Analyse und Bewertung

Alle Erkenntnisse zu Sicherheitslücken werden anhand des Prioritätsschemas für Sicherheitsprobleme (siehe unten definiert) dokumentiert und bewertet.

3. Schritt - Maßnahmen und Kontrolle

Abhängig von der Bewertung werden alle gefundenen Sicherheitslücken im Rahmen des Sicherheitsreaktionsprozesses gelöst.

Dieser besteht aus den folgenden Teilprozessen:

- Schwerwiegende Lücken werden im Rahmen des Prozesses für wichtige Updates behandelt.
- Relevante Lücken ohne höchste Dringlichkeit, die dennoch kurzfristig, d.h. in einem bereits in der Entwicklung befindlichen Release, behandelt werden müssen, werden im Rahmen des Prozesses für Supportfeatures behandelt.
- Alle verbleibenden Lücken, die kein relevantes Risiko für bestehende Funktionalität enthalten und in der Behebung mehr Aufwand benötigen, werden im Rahmen regulärer Releases behoben.

4. Schritt - Dokumentation

Alle behobenen Lücken werden in einem Sicherheitsbericht für jedes Release dokumentiert, jedoch gemäß der von der BSI empfohlenen Informationspolitik wird dieser Bericht nicht explizit an Kunden ausgeliefert.

Im Einzelnen:

1. Schritt - Identifizierung von Sicherheitsproblemen

Sicherheit analysieren und aufbauen

Das Ziel dieser Maßnahme ist es, neue Features sicher zu konstruieren. Daher wird das ATOSS R&D Team beim Entwerfen neuer Features dafür sensibilisiert, Features zu kennzeichnen, die sich auf die Sicherheit auswirken können. Das ATOSS R&D Team überprüft dies und sammelt alle potenziell sicherheitsrelevanten Probleme bis zum Beginn der Planungsphase eines Releases.

Diese Sammlung speist sich aus den folgenden Quellen:

- Von Kunden oder Partnern gemeldete Sicherheitsprobleme
- Von ATOSS beauftragte externe Sicherheitstests
- Relevante Newsletter (US Homeland Security, Heise etc.)
- Nachrichten
- Von Kunden oder Partnern durchgeführte Auditergebnisse und Penetrationstestrunden
- Intern entdeckte Probleme
- Automatische Tests (Crashtest Security, aktuell auf TAI)
- Diese wichtigen Informationsquellen werden geprüft hinsichtlich der neuesten Sicherheitsinformationen der JAVA- und Tomcat-Umgebung:

  - 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

- Relevante Sicherheitslücken führen dazu, dass auf eine neuere Version aktualisiert werden muss. Alle auf Client und Server verwendeten Drittanbieterbibliotheken werden in jedem Release mit einem Standardtool basierend auf den Maven-Abhängigkeiten gescannt. Die Ergebnisse werden analysiert und zu aktualisierende bzw. zu ersetzende Bibliotheken werden ermittelt.

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

Alle eingehenden Sicherheitsprobleme werden basierend auf dem Prioritätsschema für Sicherheitsprobleme analysiert. Bei Problemen, die für ein Release geplant sind, schlägt das ATOSS R&D Team ein „sicheres" Design vor, prüft das finale technische Design und die technische Implementierung sorgfältig, um so eine sichere und qualitativ hochwertige Implementierung sicherzustellen. Alle ggf. verbleibenden Lücken geringer Kritikalität, die nicht im laufenden Release behoben werden, werden in einem Sicherheits-Backlog gesammelt, das bei der Planung weiterer Releases weiter abgearbeitet wird.

Interne Sicherheitsaudits

Das Ziel der internen Sicherheitsaudits ist die Validierung des Sicherheitsniveaus der ATOSS Produkte innerhalb jedes neuen Releases.

Wir verfolgen dabei verschiedene Richtungen:

- Die bestehende Qualität durch Regressionstests sicherstellen. Daher verwenden wir Standardtools unserer Branche wie BURP. Falls etwas gefunden wird, werden die Funde nach dem Sicherheitsreaktionsprozess behandelt. Dieser Prozess findet während der QA-Phase jedes Releases statt.
- Der bestehende Code wird in regelmäßigen Abständen einer statischen Codeanalyse auf Basis von Veracode unterzogen.
- Prüfung behobener Sicherheitslücken: Alle Lücken, die während eines Releases geschlossen werden, werden von unseren QA-Experten zusätzlich zu den beschriebenen Tools manuell geprüft und getestet. Im

Fall des Auftretens neuer Lücken werden diese erneut anhand des Prioritätsschemas für Sicherheitsprobleme bewertet. Die im Rahmen dieser Tests gefundenen und behobenen Lücken werden im Sicherheitsbericht dokumentiert.

Externe Sicherheitsaudits

Das Ziel der externen Sicherheitsaudits ist die Validierung des Sicherheitsniveaus der ATOSS Produkte über unabhängige Prüfungen gegen ein "State-of-the-Art"-Niveau. Falls hier etwas gefunden wird, werden diese Sicherheitslücken nach dem Sicherheitsreaktionsprozess behandelt. Dieses Audit findet statt in Koordination mit unserem externen Partner, so oft wie dies der Partner – zusammen mit den Leitern des R&D Teams – aufgrund von technischen Änderungen innerhalb oder außerhalb des Unternehmens für nötig erachtet. Dabei werden auf beiden Seiten die erwarteten Änderungen und die Investitionen in Tests gegeneinander abgewogen. Der Test wird normalerweise mit dem internen Releasezyklus koordiniert, um optimale Reaktionszeiten zu ermöglichen. Das bedeutet, dass die Tests zurzeit während der QA-Phase eines neuen Releases stattfinden. Alle Funde werden anhand des Prioritätsschemas für Sicherheitsprobleme bewertet. Weiterhin wird in regelmäßigen Abständen – typischerweise einmal pro Release – mit einem weiteren Partner für die Rezertifizierung im Rahmen der SAP Integration Certification („Premium Certification as an SAP Endorsed App“) die gesamte Codebasis einer statischen Codeanalyse zur Prüfung auf Sicherheitslücken unterzogen.

Die im Rahmen der Audits gefundenen und behobenen Lücken werden ebenfalls im Sicherheitsbericht dokumentiert.

2. Schritt - Analyse und Bewertung

Die Kunden werden informiert, sobald eine Lösung für das Sicherheitsproblem existiert.

Die Analyse und Bewertung erfolgt entlang des Prioritätsschemas für Sicherheitsprobleme.

Priorität	**CVSS-Bereich (falls zutreffend)**	**Klassifizierung**	**(Sub-)Prozess Sicherheitsreaktion**	**Prozess Kundeninformation***
Niedrig	0 - 3.9	Erschwert das Benutzererlebnis / die Servicequalität Kein Risiko für Datenleck oder Datenverlust.	Behebung in einem der nächsten Releases erwägen (*Prozess für reguläre Entwicklung*)	In Neuerungen veröffentlichen, falls zutreffend
Mittel	4 - 6.9	z. B. Risiko eines Lesezugriffs auf nicht berechtigte Daten	Im nächsten Release beheben (*Prozess für Support Features*)	In Neuerungen veröffentlichen, falls zutreffend
Hoch	7 - 8.9	z. B. Risiko eines Schreibzugriffs auf nicht berechtigte Daten	Sofort beheben (*Prozess für wichtige Updates)*	Betroffene Kunden identifizieren und Update empfehlen
Kritisch	9 - 10	z. B. Risiko eines Lese-/Schreibzugriffs über die Grenzen der ATOSS Systeme hinaus	Sofort beheben (*Prozess für wichtige Updates)*	Betroffene Kunden identifizieren und Update empfehlen

Bei der effektiven Priorisierung werden die Risiken und die Wahrscheinlichkeit, dass die Sicherheitslücke in den ATOSS Produkten tatsächlich ausgenutzt werden kann, berücksichtigt.

3. Schritt - Maßnahmen und Kontrolle

Prozess für reguläre Softwareentwicklung

Dieser Prozess wird für Sicherheitsprobleme der Priorität "Niedrig" verwendet. Diese Einstufung erfordert keine kurzfristige Behebung. Daher wird die Behebung im Rahmen der regulären Release-Entwicklung entsprechend eingeplant. Sie wird dem Backlog der Features hinzugefügt, die aufgrund der Analyse "Sicherheit aufbauen" des nächsten Releases (siehe oben) berücksichtigt werden. Die Planung und Behebung dieser Sicherheitsprobleme folgt dem viermonatigen Standard-Releasezyklus.

Prozess für Support Features

Dieser Prozess wird für Sicherheitsprobleme der Priorität "Mittel" verwendet. Er ist in das Release integriert. Mittels dieses Prozesses werden diese Sicherheitsprobleme behandelt, die auch noch im aktuell in der Entwicklung befindlichen Releases behandelt werden müssen.

Prozess für wichtige Updates

Dieser Prozess ist für "kritische" und als "hoch" eingestufte Sicherheitsprobleme identisch.

Alle Teammitglieder in allen relevanten Fachabteilungen kennen diesen Prozess. Die Behandlung eines Sicherheitsproblems beginnt an dem Arbeitstag, an dem es erkannt und entsprechend klassifiziert wurde, um so die schnellstmögliche Lösung zu garantieren. Die zu erarbeitende Lösung enthält eine detaillierte Beschreibung der effektiven internen Behandlung, die Erstellung von Build- oder Patch-Versionen, eine Kommunikationsstrategie für die betroffenen Kunden und ggf. ein Supportangebot, falls der Kunde dies benötigt. Der Prozess der Behebung wird sorgfältig dokumentiert und nachverfolgt, bis alle betroffenen Kunden zumindest über das Problem und seine Behebung informiert wurden.

Kontrolle und Eskalation

Für alle oben genannten Prozesse sind verantwortliche Rollen definiert, die die Maßnahmen zur Behebung des Sicherheitsproblems überwachen. Beim Prozess für Support Features und reguläre Softwareentwicklung ist der Release-Manager verantwortlich. Bei wichtigen Updates ist der Leiter der Produktentwicklung verantwortlich. Falls eine Maßnahme nicht den gewünschten Effekt zeigt, wird ein Eskalationsbericht an die Geschäftsleitung für weitere Maßnahmen und Entscheidungen verfasst. Zusätzlich existiert beim ATOSS R&D Team ein Feedback- und Prüfprozess, in dessen Rahmen nach jedem kritischen Vorfall Möglichkeiten zur Verbesserung untersucht werden.

4. Schritt - Dokumentation

Für jedes Release dokumentiert das ATOSS I&D Team einen internen Sicherheitsbericht, der die oben genannten Ergebnisse der Analyse, die Bewertung, die Maßnahmen und Kontrollen zusammenfasst.

ATOSS.COM

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

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

ATOSS Software AG
Luggwegstr. 9
8048 Zürich
Schweiz
T +41 44 501 53 00

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

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

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

Besuchen Sie für weitere Information unsere Website www.atoss.com oder schicken Sie uns eine E-Mail an internet@atoss.com