R&D-Sicherheitsprozess für ASE/S und ATC

Version: 2.03

Letztes Bearbeitungsdatum: 21.03.2024

Dieses Dokument fokussiert auf die ATOSS Hauptprodukte ASE/S und ATC. Es beinhaltet keine Sicherheitsaspekte in Bezug auf

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

Inhalt

0. Vorwort

Sicherheit ist unsere Mission

ATOSS nimmt die Sicherheit ihrer Produkte sehr ernst und verfügt über einen umfassenden und sicheren Softwareentwicklungsprozess und klare Qualitäts- und Sicherheitsstandards für die Softwareentwicklung. Ein spezieller Security Response Process ist der sichtbarste Beweis für unser Engagement. Das ATOSS R&D Team ist für die Untersuchung aller gemeldeten Sicherheitslücken verantwortlich und arbeitet eng mit den Entdeckern der Schwachstellen zusammen, um Patches bereitzustellen. ATOSS informiert die Kunden über die Patches und deren Wichtigkeit. Integrität und Sicherheit von Geschäftsabläufen sind für Unternehmen aller Branchen von entscheidender Bedeutung. Daher stellt ATOSS als Anbieter von Unternehmenssoftware das höchstmögliche Maß an Sicherheit für ihre Produkten sicher.

ATOSS unterstützt die verantwortungsvolle Offenlegung von Sicherheitslücken.

Wenn Sie eine Sicherheitslücke in einem unserer Software-produkte entdecken - entweder in der aktuellen oder in einer früheren Produktversion – melden Sie das Problem auf https://www.atoss.com/de/sicherheit/sicherheitsproblem-melden.

Geben Sie ATOSS ausreichend Zeit, Patches zu entwickeln

- Die Behebung von Sicherheitslücken kann ein langwieriger und mühsamer Prozess sein, da wir einen Patch entwickeln, seine Kompatibilität mit allen relevanten Softwareversionen sicherstellen, umfassende Tests durchführen, um sicherzustellen, dass die Korrekturen gut funktionieren und keine Nebenwirkungen haben, und ihn unseren Kunden zur Verfügung stellen.
- Als Anbieter von Unternehmenssoftware stellen wir nicht nur für die neueste Version, sondern auch für viele ältere Versionen unserer Softwareprodukte Sicherheitskorrekturen bereit. Das bedeutet, dass wir praktikable Patches für eine breite Palette von Produktversionen entwickeln und gründlich testen müssen, was einige Zeit in Anspruch nehmen kann.

Veröffentlichen Sie Schwachstellen erst dann, wenn ATOSS Kunden Zeit hatten, diese zu beheben.

Das Ausrollen von Patches für ATOSS Produkte ist in der Regel komplizierter als ein Software-Upgrade auf einem Consumer-PC. Je nach Art der Schwachstelle erfordert die Bereitstellung von Patches oder Updates in einigen Fällen Konfigurations- oder Bereitstellungsaufgaben im Hinblick auf kundeninterne Einschränkungen oder Prozesse. Einige unserer Kunden folgen zum Beispiel regelmäßigen Patch-Zyklen. Unter Berücksichtigung dieser Umstände bitten wir alle Sicherheitsforscher, den ATOSS Kunden ausreichend Zeit für die Implementierung von Patches in ihre Systeme zu geben.

Als Faustregel empfehlen wir, eine Implementierungszeit von drei Monaten beim Kunden einzuhalten, sobald der Patch von ATOSS veröffentlicht wurde. Mit Rücksicht auf die Interessen unserer Kunden bitten wir alle Sicherheitsforscher, während dieser Zeit keine Informationen oder Tools zu verbreiten, mit denen die Schwachstelle ausgenutzt werden kann.

Bitte informieren Sie unser R&D-Team auch über alle Ihre bevorstehenden öffentlichen Stellungnahmen und externen Präsentationen mit ATOSS-Produktsicherheitsinhalten, einschließlich der beabsichtigten Inhalte, mindestens 3 Wochen im Voraus.

1. Wichtigste Normen und Empfehlungen

ATOSS nutzt relevante Quellen, um Informationen zu Sicherheitsfragen und Maßnahmen zum Schutz von Anwendungen zu sammeln. Neben Informationen, die von Drittanbietern von Produkten, die von ATOSS verwendet werden (wie ORACLE usw.), veröffentlicht werden, konzentrieren wir uns hauptsächlich auf die folgenden international vereinbarten Quellen:

- BSI Bundesamt für Sicherheit in der IT: https://www.bsi.bund.de/
- OWASP Open Worldwide Application Security Project: Open Worldwide Application Security Project

Deren Veröffentlichungen werden kontinuierlich und gründlich analysiert. Aspekte, die auf die ATOSS Produkte anwendbar sind, werden im Rahmen der R&D-internen Produktentwicklung detailliert untersucht und mit Maßnahmen belegt. Für sicherheitsrelevante Fälle wird der ATOSS Security News (https://www.atoss.com/en/security/security-news) Feed aktualisiert. Für Details siehe unten.

2. Überblick über den Sicherheitsprozess

Der Prozess folgt den Aspekten des Standard-Risikomanagement-Prozesszyklus:

Identifizierung: Der ATOSS interne Sicherheitsprozess hat drei Komponenten, die sich gegenseitig ergänzen:

- Gemeinsam mit einem externen Partner gehen wir das Hauptproblem der Sicherheit an: Kreativität und "Hacker-"Wissen. In regelmäßigen Abständen - abhängig von Änderungen in der Technologie unserer Anwendung oder Erkenntnissen unseres Partners - definieren wir Testzyklen während der QA-Phase des jeweiligen Releases. In der Regel werden diese externen Tests einmal jährlich durchgeführt. Falls erforderlich, werden sie auch häufiger durchgeführt ***(Externes Sicherheitsaudit)***.
- ATOSS überprüft unsere Sicherheit regelmäßig intern während der speziellen QA-Phase innerhalb unseres 4-monatigen Software-Release-Zyklus durch sorgfältige interne Sicherheitstests (Regressionstests) auf der Grundlage von Industriestandard-Tools und durch manuelle Tests neuer sicherheitsrelevanter Funktionen ***(Interner Sicherheitstest)***.
- ATOSS konstruiert Sicherheit, indem sie sichere Software unter Berücksichtigung der oben genannten Quellen implementiert. **(Security-by-design)**.

Analysieren und Bewerten: Alle Feststellungen werden dokumentiert und anhand des ***Prioritätsschemas für Sicherheitsprobleme*** (siehe unten) bewertet.

Maßnahmen und Kontrolle: Je nach Einstufung werden alle Feststellungen im Rahmen des ***Security Response Process*****,** der aus den folgenden Teilprozessen besteht, wirksam behandelt:

- Dringende Befunde werden über den ***Prozess der wichtigen Aktualisierung behandelt*****.**
- Relevante Erkenntnisse ohne höchste Dringlichkeit, die dennoch in einem bereits in Entwicklung befindlichen Release über den ***Support Feature Process*** behandelt werden müssen***.***
- Alle Erkenntnisse, die einen höheren Aufwand erfordern, ein relevantes Risiko für die bestehende Funktionalität darstellen oder nicht kritisch sind, werden im Rahmen des ***regulären Freigabeprozess.***

Dokumentation: Alle Probleme und die damit verbundenen Ergebnisse werden in einem ***Sicherheitsbericht*** dokumentiert, der mit jeder neuen Version aktualisiert wird, aber gemäß der Informationspolitik des BSI nicht explizit an die Kunden geliefert wird.

3. Identifizierung von Sicherheitsproblemen

Externes Sicherheitsaudit

Ziel dieses Audits ist die Validierung des Sicherheitsniveaus der ATOSS Produkte durch unabhängige Prüfungen gegen einen "State-of-the-Art"-Stand ("externer Penetrationstest"). Sollten Feststellungen getroffen werden, so werden diese gemäß dem ***Security Response Process*** behandelt. Dieser Audit findet in Abstimmung mit unserem externen Partner so oft statt, wie der Partner - gemeinsam mit den Leitern der R&D-Abteilung - die Notwendigkeit aufgrund technischer Veränderungen in der Innen- oder Außenwelt sieht. Dies geschieht in einem ausgewogenen Verhältnis zwischen erwarteten Änderungen und Testaufwand auf beiden Seiten. Der Test wird in der Regel mit dem internen Release-Zyklus abgestimmt, um optimale Reaktionszeiten zu ermöglichen. Das bedeutet, dass die Tests derzeit während der QA-Phase einer neuen Version stattfinden. Alle Ergebnisse werden nach dem ***Security Issue Priority Scheme*** bewertet.

Das Audit liefert ein Prüfergebnis, das in den ***Sicherheitsbericht*** integriert wird, der für jedes Release aktualisiert wird (siehe unten).

Tests zur internen Sicherheit

Ziel dieses Tests ist es, das Sicherheitsniveau der ATOSS Produkte in jedem neuen Release zu validieren. Wir gehen dabei in zwei Richtungen:

1. Sichern Sie die bestehende Qualität durch Regressionstests. Dazu verwenden wir Industriestandard-Tools wie BURP. Falls es zu Feststellungen kommt, werden diese gemäß ***Sicherheits-Reaktions-Prozess behandelt.*** Dieser Prozess findet während der QA-Phase jeder Version statt.
2. Testen Sie neue Sicherheitserkenntnisse: Alle Erkenntnisse, die während einer Veröffentlichung umgesetzt werden, werden von unseren QA-Experten manuell geprüft und getestet. Wenn es Feststellungen gibt, werden

sie erneut nach dem ***Prioritätsschema für Sicherheitsprobleme*** bewertet.

Der Test liefert auch ein Testergebnis, das in den ***Sicherheitsbericht*** integriert wird, der für jede Version aktualisiert wird (siehe unten).

Analyse und Security-by-design

Das Ziel dieser Maßnahme ist es, neue Funktionen auf sichere Weise zu entwickeln. Daher werden alle Teammitglieder bei der Entwicklung neuer Funktionen sensibilisiert, alle Funktionen zu markieren, die Auswirkungen auf die Sicherheit haben könnten. Das R&F-Team prüft dies und sammelt alle potenziell sicherheitsrelevanten Aspekte bis zum Beginn der Planungsphase einer neuen Version. Diese Sammlung wird aus den folgenden Quellen gespeist:

- Gemeldete Sicherheitsprobleme von Kunden oder Partnern
- Externe Sicherheitstests im Auftrag von ATOSS
- Static Application Security Testing auf der Grundlage des SAST-Analyzers von Veracode - eine Form der statischen Code-Analyse, bei der ein ASE/S-Code auf Sicherheitslücken gescannt wird
- Einschlägige Newsletter (US Homeland Security, Heise, etc.)
- Öffentliche Nachrichten
- Audit-Ergebnisse und Ergebnisse von Penetrationstests, die von Kunden oder Partnern durchgeführt wurden
- Intern entdeckte Probleme
- Automatische Tests
- Diese Hauptinformationsquellen werden auf die neuesten Sicherheitsinformationen der **JAVA- und Tomcat-Umgebung** überprüft:
    - https://www.oracle.com/security-alerts/
    - https://www.cisa.gov/
    - https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-23642/Oracle-Openjdk.html
    - https://tomcat.apache.org/security-9.html
    - Einschlägige Sicherheitslücken führen zu einer Aufforderung zur Aktualisierung auf eine neuere Version.

- Alle **Bibliotheken von Drittanbietern,** die auf der Client- und Serverseite verwendet werden, werden bei jeder Veröffentlichung mit einem Standardwerkzeug (https://owasp.org/www-project-dependency-check/) auf der Grundlage der Maven-Abhängigkeiten gescannt. Die Ergebnisse werden analysiert und die zu aktualisierenden oder zu ersetzenden Bibliotheken werden ermittelt.

Alle eingehenden Sicherheitsprobleme werden auf der Grundlage des **Prioritätsschemas für Sicherheitsfragen** analysiert. Für Probleme, die für eine neue Version geplant sind, macht die technische Abteilung einen klaren Entwurfsvorschlag und prüft den endgültigen Entwurf und die technische Implementierung sorgfältig, um eine sichere und qualitativ hochwertige Implementierung zu gewährleisten. Alle anderen Probleme werden in einem Sicherheitsbestand gesammelt, der für die Planung weiterer Versionen verwendet wird.

4. Analyse und Bewertung entlang der Sicherheitsfrage Prioritätsschema

Priorität	**CVSS-Bereich (falls zutreffend)**	**Klassifizierung**	**Sicherheitsreaktion (Sub) Prozess**	**Kundeninformationsprozess ***
Niedrig	0 - 3.9	Beeinträchtigung der Benutzererfahrung/Dienstqualität Kein Risiko von Datenlecks oder Datenverlust.	Behebung in einer der nächsten Versionen in Betracht ziehen (*regulärer Entwicklungsprozess*)	Gegebenenfalls in den Versionshinweisen veröffentlichen
Mittel	4 - 6.9	z.B. Risiko des Lesezugriffs auf nicht autorisierte Daten.	Behebung in einer kommenden Version (*Support Feature Process*)	Gegebenenfalls in den Versionshinweisen veröffentlichen
Hoch	7 - 8.9	z.B. Risiko des Schreibzugriffs auf nicht autorisierte Daten	Sofort beheben (*Wichtiger Update-Prozess*)	Identifizierung der betroffenen Kunden und Empfehlung eines Updates (wichtiger Update-Prozess)

Kritisch	9 - 10	z.B. Risiko des Lese-/Schreibzugriffs über die ATOSS Systemgrenzen hinaus.	Sofort beheben (*Wichtiger Update-Prozess*)	Identifizieren Sie betroffene Kunden und empfehlen Sie dringend eine Aktualisierung (wichtiger Aktualisierungsprozess)

Die effektive Priorisierung berücksichtigt die Risiken und die Wahrscheinlichkeit, dass die Schwachstelle im ASE/S oder ATC tatsächlich ausgenutzt werden kann.

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

5. Maßnahmen entlang des Security Response Process

Wichtiger Updateprozess

Diese Lösung wird in gleicher Weise für "kritische" und "hohe" funktionale Probleme verwendet. Alle Teammitglieder in allen relevanten Abteilungen sind mit diesem Verfahren vertraut. Die Behandlung des Sicherheitsproblems beginnt an dem Arbeitstag, an dem es entdeckt und entsprechend eingestuft wurde, um die schnellstmögliche Lösung zu gewährleisten. Sie beinhaltet eine detaillierte Beschreibung der effektiven internen Behandlung, die Erstellung von Update- oder Patch-Versionen, eine Kommunikationsstrategie gegenüber den betroffenen Kunden und ein Angebot für Support, falls der Kunde diesen benötigt. Der Prozess wird sorgfältig dokumentiert und nachverfolgt, bis alle betroffenen Kunden zumindest das Wissen über das Problem und seine Behebung bestätigt haben.

Unterstützung des Feature-Prozesses

Dieser Prozess wird für Sicherheitsprobleme der Priorität "Mittel" verwendet. Er ist in die Version integriert und kümmert sich um Sicherheitsprobleme von geringerer Kritikalität, die nicht nur in der nächsten Version behandelt werden müssen, sondern auch in Versionen, die sich gerade in der Entwicklung befinden. Das heißt, diese Fälle werden nicht auf eine spätere Version verschoben, sondern sind kritisch genug, um die Planung der aktuell entwickelten Version zu ändern. Sie können diese Funktion auch als "Änderung" der aktuellen Version bezeichnen.

Regulärer Entwicklungsprozess

Dies wird für Sicherheitsprobleme mit der Priorität "Niedrig" verwendet. Dies bedeutet, dass die Funktion nicht in kurzer Zeit bereitgestellt werden muss. Daher wird die Implementierung in einer Standardform geplant. Sie wird dem Backlog der Funktionen hinzugefügt, die aufgrund der "Security-by-design"-Analyse für die nächste Version in Betracht gezogen werden (siehe oben).

Die Planung und Behebung dieser Sicherheitsprobleme folgt dem üblichen 4-monatigen Veröffentlichungszyklus. Alle in einem Release geplanten Probleme werden in einer Tabelle mit der folgenden Struktur gesammelt und dokumentiert. Alle Funktionen, die in einem Release geplant und ausgeliefert werden, werden in demselben Format dokumentiert, das auch Teil des ***Sicherheitsberichts ist.***

Datum	**Externe Quelle**	**Entscheidung: Kein Risiko / nicht relevant**	**Risiko**	**Geplant für die Veröffentlichung**
	<Quelle 1>	<Grund>	<Link zu Jira/Bugzilla-Problem. Setzen Sie die Jira-Flags 'Sicherheitsproblem' und 'Sicherheitsrelevant'>	Version

6. Kontrolle und Eskalation

Alle oben genannten Prozesse haben eine klare verantwortliche Rolle, die die Durchführung der Maßnahme zur Behebung des Sicherheitsproblems kontrolliert. Für wichtige Aktualisierungen ist der Leiter der Produktentwicklung zuständig, für den Support-Feature-Prozess und den regulären Entwicklungsprozess ist der Release-Manager verantwortlich. Für den Fall, dass eine Maßnahme nicht die beabsichtigte Wirkung zeigt, gibt es einen Eskalationsbericht an den Vorstand für weitere Maßnahmen und Entscheidungen. So wird sichergestellt, dass auch bei Problemen die effektivsten Maßnahmen ergriffen werden. Weiterhin ist als Standardprozess in R&D ein Feedback- und Review-Prozess etabliert, der auf Verbesserungsmöglichkeiten prüft. Das heißt, auch dieser Sicherheitsprozess wird in einem Release basierten Kreislauf überprüft.

7. Überwachung: Der Sicherheitsbericht

Für jede Freigabe gibt es einen internen Sicherheitsbericht für den ASE/S und den ATC, in dem die oben genannten Ergebnisse der Analyse, der Bewertung, der Maßnahmen und der Ergebnisse zusammengefasst werden. Genauer gesagt enthält er die folgenden Abschnitte:

1. Merkmale, die im Rahmen des regulären Entwicklungsprozesses implementiert wurden, in Form einer Tabelle mit Beschreibung und Testergebnissen
2. Ergebnisse der internen Sicherheitsregressionstests und Maßnahmen
3. Ergebnisse der externen Sicherheitsregressionstests und Maßnahmen
4. Vielfältige Aspekte - wie Dokumentation externer Befunde und daraus resultierende wichtige Aktualisierungsergebnisse