ATOSS

R&D-Sicherheitsprozess für ATOSS Staff Efficiency Suite und ATOSS Time Control | Extern

Version: 2.00
Stand: 18.03.2020

Haftungsausschluss: Das Dokument konzentriert sich auf die ATOSS Hauptprodukte ATOSS Staff Efficiency Suite und ATOSS Time Control. Es beinhaltet keine Sicherheitsaspekte im Hinblick auf

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

Inhalt

0. Vorwort

Sicherheit ist uns wichtig

ATOSS nimmt die Sicherheit seiner Produkte sehr ernst. Dazu verfügen wir über einen umfassenden Prozess für einen sicheren Softwareentwicklungs-Lebenszyklus sowie klare Qualitäts- und Sicherheitsstandards für die Softwareentwicklung. Der sichtbarste Beweis für unser Engagement ist ein etablierter dedizierter Prozess zur Reaktion auf Sicherheitsprobleme. Das ATOSS R&D-Team ist dafür verantwortlich, alle gemeldeten Sicherheitslücken zu untersuchen. Dabei arbeitet es eng mit den Personen an der Bereitstellung von Patches, die die Lücken gemeldet haben. ATOSS informiert die Kunden über die Patches und deren Relevanz. Da die Integrität und Sicherheit des Geschäftsbetriebs für alle Unternehmen in allen Branchen essenziell ist, setzt sich ATOSS als Anbieter von Business-Software unbedingt dafür ein, in seinen Produkten die höchstmögliche Sicherheitsebene aufrechtzuerhalten.
ATOSS unterstützt die verantwortungsbewusste Offenlegung von Sicherheitslücken. Wenn Ihnen in einem unserer Softwareprodukte eine Sicherheitslücke aufgefallen ist – entweder in der neuesten oder in einer älteren Produktversion – teilen Sie uns das bitte mit unter security@atoss.com.

Geben Sie ATOSS genügend Zeit zur Entwicklung passender Korrekturen

- Das Beheben von Sicherheitslücken kann langwierig und beschwerlich sein: Wir entwickeln einen Patch, stellen sicher, dass er mit allen relevanten Softwareversionen kompatibel ist, führen umfassende Tests durch, damit die Korrekturen ohne Nebenwirkungen und fehlerfrei laufen, und stellen ihn unseren Kunden zur Verfügung.
- Als Anbieter von Business-Software bieten wir nicht nur für die neueste Version Sicherheitskorrekturen an, sondern auch für viele ältere Versionen unserer Softwareprodukte. Das bedeutet, dass wir brauchbare Patches für eine große Palette an Produktversionen entwickeln und gründlich testen müssen. Das braucht Zeit.

Veröffentlichen Sie keine Sicherheitslücken, bevor ATOSS Kunden Zeit hatten, Korrekturen bereitzustellen

Die Bereitstellung von Patches für ATOSS Produkte ist üblicherweise komplizierter als ein Softwareupgrade auf einem Kunden-PC. Je nach Art der Sicherheitslücke sind für die Bereitstellung von Patches bzw. Updates in manchen Fällen Konfigurations- bzw. Bereitstellungsaufgaben hinsichtlich kundeninterner Beschränkungen oder Prozesse erforderlich. Einige unserer Kunden folgen beispielsweise regulären Patchzyklen. Unter Berücksichtigung dieser Umstände bitten wir alle Sicherheitsforscher, ATOSS Kunden genügend Zeit dafür zu geben, Patches in ihren Systemen zu implementieren. Als Faustregel schlagen wir vor, den

Kunden eine Implementierungszeit von drei Monaten zuzugestehen, sobald der Patch von ATOSS freigegeben wurde. Unter Berücksichtigung unserer Kundeninteressen bitten wir alle Sicherheitsforscher, keine Informationen oder Tools in Umlauf zu bringen, die in dieser Zeit dazu beitragen könnten, die Sicherheitslücke auszunutzen.

Bitte informieren Sie außerdem das R&D-Team mindestens drei Wochen im Voraus über alle Ihre zu veröffentlichenden Sicherheitshinweise und anstehenden externen Präsentationen mit Sicherheitsinhalt aus ATOSS Produkten in einer E-Mail an security@atoss.com, einschließlich des voraussichtlichen Inhalts.

1. Hauptstandards und Empfehlungen

ATOSS verwendet relevante Quellen zum Sammeln von Informationen bezüglich Sicherheitsproblemen und Maßnahmen, um die Anwendungen zu schützen. Neben von Drittanbietern veröffentlichten Informationen, deren Produkte ATOSS verwendet (z. B. ORACLE etc.), konzentrieren wir uns hauptsächlich auf die folgenden international vereinbarten Quellen:

- 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

Deren Veröffentlichungen werden ständig und gründlich analysiert. Aspekte, die die ATOSS Produkte betreffen, werden während des R&D-internen Produktentwicklungszyklus detailliert untersucht. Davon werden dann entsprechende Maßnahmen abgeleitet. Details siehe unten.

2. Überblick über den Sicherheitsprozess

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

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

- Zusammen mit einem externen Partner sprechen wir das Hauptsicherheitsproblem an: Kreativität und auf "Hacker" bezogenes Wissen. Regelmäßig, abhängig von den Änderungen bei der Technologie unserer Anwendung oder den Funden unseres Partners, definieren wir während der QA-Phase des ermittelten Releases Testzyklen. Normalerweise finden diese externen Tests jährlich statt. Falls nötig werden sie häufiger durchgeführt (*externes Sicherheitsaudit*).
- ATOSS prüft seine Sicherheit regelmäßig intern während der dedizierten QA-Phase innerhalb unseres viermonatigen Softwarereleasezyklus durch einen sorgfältigen internen Sicherheitstest (Regressionstest), basierend auf den Standardtools der Branche und auf manuellen Tests neuer sicherheitsrelevanter Features (*interner Sicherheitstest*).
- ATOSS baut Sicherheit auf durch die Implementierung sicherer Software hinsichtlich der oben genannten Quellen (*Sicherheit aufbauen*).

Analyse und Bewertung: Alle Funde werden anhand des *Prioritätsschemas für Sicherheitsprobleme* (siehe unten) dokumentiert und bewertet.

Maßnahmen und Kontrolle: Abhängig von der Bewertung werden alle Funde effektiv über den *Sicherheitsreaktionsprozess* behandelt, der sich aus den folgenden Unterprozessen zusammensetzt:

- Wichtige Funde werden über den *Prozess für wichtige Updates* behandelt.
- Relevante Funde ohne die höchste Dringlichkeit, die dennoch in einem bereits in der Entwicklung befindlichen Release behandelt werden müssen, werden im *Prozess für Supportfeatures* behandelt.
- Alle Funde, die mehr Aufwand erfordern, ein relevantes Risiko für bestehende Funktionalität enthalten oder nicht kritisch sind, werden über den *Prozess für reguläre Releases* angesprochen.

Dokumentation: Alle Probleme und die damit verbundenen Ergebnisse werden in einem ***Sicherheitsbericht*** dokumentiert, der mit jedem Release aktualisiert wird, jedoch laut der BSI-Informationspolitik nicht explizit an Kunden ausgeliefert wird.

3. Identifizierung von Sicherheitsproblemen

Externer Sicherheitsaudit

Das Ziel dieses Audits ist die Validierung des Sicherheitsniveaus der ATOSS Produkte über unabhängige Prüfungen gegen ein "State-of-the-Art"-Niveau ('externer Penetrationstest'). Falls hier etwas gefunden wird, werden die Funde

nach dem *Sicherheitsreaktionsprozess* behandelt. Dieses Audit findet statt in Koordination mit unserem externen Partner, so oft wie der Partner – zusammen mit den Leitern der R&D-Abteilung – dies 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.

Das Audit liefert ein Testergebnis, das in den *Sicherheitsbericht* eingebunden wird. Dieser Bericht wird für jedes Release aktualisiert (siehe unten).

Interne Sicherheitstests

Das Ziel dieses Tests ist die Validierung des Sicherheitsniveaus der ATOSS Produkte innerhalb jedes neuen Releases. Wir verfolgen dabei zwei Richtungen:

1. 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.
2. Neue Sicherheitsfunde testen: Alle Funde, die während eines Releases implementiert werden, werden von unseren QA-Experten manuell geprüft und getestet. Im Fall von Funden werden diese erneut anhand des *Prioritätsschemas für Sicherheitsprobleme* bewertet.

Der Test liefert ebenfalls ein Testergebnis, das in den *Sicherheitsbericht* eingebunden wird. Dieser Bericht wird für jedes Release aktualisiert (siehe unten).

Sicherheit analysieren und aufbauen

Das Ziel dieser Maßnahme ist es, neue Features sicher zu konstruieren. Daher werden alle Teammitglieder beim Entwerfen neuer Features dafür sensibilisiert, alle Features zu kennzeichnen, die sich auf die Sicherheit auswirken könnten. Das 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 Penetrationstestunde
- Intern entdeckte Probleme
- Automatische Tests (CrashtestSecurity, 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 (https://owasp.org/www-project-dependency-check/) basierend auf den Maven-Abhängigkeiten gescannt. Die Ergebnisse werden analysiert und zu aktualisierende bzw. zu ersetzende Bibliotheken werden ermittelt.
- 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 die Technologieabteilung einen klaren Entwurf vor, prüft den finalen Entwurf und die technische Implementierung sorgfältig, um eine sichere und qualitativ hochwertige Implementierung sicherzustellen. Alle anderen Probleme werden in einem Sicherheits-Backlog gesammelt, das bei der Planung weiterer Releases wiederverwendet wird.

4. Analyse und Bewertung entlang des Prioritätsschemas für Sicherheitsprobleme

Priorität	**CVSS-Bereich (falls zutreffend)**	**Klassifizierung**	**(Unter-)Prozess Sicherheits-reaktion**	**Prozess Kunden-information***
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 (Prozess für wichtige Updates)
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 (Prozess für wichtige Updates)

Bei der effektiven Priorisierung werden die Risiken und die Wahrscheinlichkeit, dass die Sicherheitslücke in der ATOSS Staff Efficiency Suite bzw. der ATOSS Time Control tatsächlich ausgebeutet werden kann, berücksichtigt.

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

5. Maßnahmen entlang des Sicherheitsreaktionsprozesses

Prozess für wichtige Updates

Diese Lösung ist für "kritische" und "hohe" funktionale Probleme identisch. Allen Teammitgliedern in allen relevanten Abteilungen ist dieser Prozess bewusst. Die Handhabung des Sicherheitsproblems beginnt an dem Arbeitstag, an dem es erkannt und entsprechend klassifiziert wurde, um die schnellstmögliche Lösung zu garantieren. Sie enthält eine detaillierte Beschreibung der effektiven internen Behandlung, die Erstellung von Build- oder Patchversionen, eine Kommunikationsstrategie für die betroffenen Kunden und ein Supportangebot, falls der Kunde dies benötigt. Der Prozess wird sorgfältig dokumentiert und nachverfolgt, bis alle betroffenen Kunden zumindest ihre Kenntnis des Problems und seiner Behebung bestätigt haben.

Prozess für Supportfeatures

Dieser Prozess wird für Sicherheitsprobleme der Priorität "Mittel" verwendet. Er ist in das Release integriert und kümmert sich um Sicherheitsprobleme von geringer Relevanz, die nicht nur im nächsten Release, sondern auch in den aktuell in der Entwicklung befindlichen Releases behandelt werden müssen. Das heißt, dass diese Fälle nicht in ein späteres Release verschoben werden dürfen, sondern kritisch genug sind, um die Planung des aktuell entwickelten Releases zu ändern. Dieses Feature kann man auch als "Änderung" des aktuellen Releases bezeichnen.

Prozess für reguläre Entwicklung

Dieser Prozess wird für Sicherheitsprobleme der Priorität "Niedrig" verwendet. Das heißt, dass das Feature nicht kurzfristig ausgeliefert werden muss. Daher wird die Implementierung dem Standard entsprechend geplant. 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 Standardreleasezyklus. Alle in einem Release geplanten Probleme werden gesammelt und in einer Tabelle mit dem folgenden Aufbau dokumentiert. Alle Features, die in einem Release geplant sind und ausgeliefert werden, werden im gleichen Format dokumentiert, das Teil des ***Sicherheitsberichts*** ist.

Datum	Externe Quelle	Entscheidung: Kein Risiko / Nicht relevant	Risiko	Geplant für Release
	<Quelle 1>	<Grund>	<Link zu Jira/Bugzilla-Fall. Jira-Flags 'Security issue' und 'Relevant for security' setzen>	Version

6. Kontrolle und Eskalation

Alle oben genannten Prozesse besitzen eine klare verantwortungsvolle Rolle, die die Erfüllung der Maßnahme zur Behebung des Sicherheitsproblems kontrolliert. Bei wichtigen Updates ist der Leiter der Produktentwicklung verantwortlich, beim Prozess für Supportfeatures und reguläre Entwicklung ist es der Release-Manager. Falls eine Maßnahme nicht den gewünschten Effekt zeigt, wird ein Eskalationsbericht an die Geschäftsleitung für weitere Maßnahmen und Entscheidungen verfasst. Dadurch werden selbst bei Problemen die effektivsten Maßnahmen sichergestellt. Des Weiteren ist als Standardprozess bei R&D ein Feedback- und Prüfprozess etabliert, der nach Möglichkeiten zur Verbesserung sucht. Das bedeutet, dass der Sicherheitsprozess auch in einem releasebasierten Zyklus geprüft wird.

7. Überwachung: Der Sicherheitsbericht

Für jedes Release der ATOSS Staff Efficiency Suite und der ATOSS Time Control gibt es einen internen Sicherheitsbericht, der die oben genannten Ergebnisse der Analyse, die Bewertung, die Maßnahmen und die Ergebnisse zusammenfasst. Konkret enthält er die folgenden Abschnitte:

1. Durch den Prozess für reguläre Entwicklung implementierte Features als Tabelle mit Beschreibung und Testergebnissen
2. Funde des internen Sicherheitsregressionstests und Maßnahmen
3. Funde von externen Sicherheitsregressionstests und Maßnahmen
4. Diverse Aspekte wie die Dokumentation externer Funde und daraus resultierende Ergebnisse wichtiger Updates