Protégez vos données en restant à jour avec Toad® by Quest

Fiche technique sur les standards de sécurité logicielle intégrés à Toad for Oracle

Par Julie Hyman, responsable de produit senior, et Ryan Crochet, responsable marketing produits senior, Quest Software

Dans le contexte actuel de la prolifération des cybermenaces, il est essentiel pour les administrateurs informatiques de définir des règles claires concernant les logiciels autorisés sur les ordinateurs et sur le réseau, indépendamment de l'architecture ou des protocoles de sécurité en place. La multiplication des attaques par rançongiciel Exotic, la hausse des activités malveillantes, l'habitude qu'ont les entreprises de s'appuyer sur un éventail plus vaste de logiciels et d'applications pour atteindre leurs objectifs professionnels : autant de facteurs qui requièrent un engagement proactif avec une main de fer en matière de gestion des logiciels. Pour protéger les actifs numériques de votre organisation, respectez au minimum les priorités suivantes :

1. Seuls des logiciels sécurisés doivent être installés.
2. Les logiciels sont mis à jour en continu pour maintenir la sécurité des systèmes.

Dans cette fiche technique, vous allez découvrir comment respecter ces exigences, qui vous garantiront la sécurité des logiciels de votre chaîne logistique.

Poursuivez la lecture pour en savoir plus sur les sujets suivants :

- **Qu'est-ce que la sécurité de la chaîne logistique logicielle et pourquoi est-ce important pour vous ?**
- **L'importance de maintenir ses logiciels à jour**
- **Contrôles de sécurité essentiels qui permettent à Toad de vous protéger**

SÉCURITÉ DE LA CHAÎNE LOGISTIQUE LOGICIELLE

Dans le contexte de la chaîne logistique logicielle, la sécurité fait référence à l'intégrité, à la confidentialité et à la disponibilité des composants logiciels et de leurs dépendances tout au long du cycle de développement des logiciels, de leur création à leur déploiement. C'est primordial, car des composants logiciels compromis peuvent nuire aux entreprises et à leurs clients. Quand la chaîne logistique logicielle est protégée par des mesures de sécurité efficaces, les risques sont réduits grâce à une visibilité, un contrôle et une garantie accrus tout au long du processus.

SÉCURITÉ DES DONNÉES ET TOAD

Toad by Quest est un environnement de développement intégré (IDE) qui permet aux développeurs et aux administrateurs de base de données de créer, gérer et maintenir des bases de données, rôles et utilisateurs compris. Ainsi, si un pirate parvenait à accéder à la session Toad d'un utilisateur, il pourrait exécuter des commandes de base de données non autorisées, voler des données sensibles ou même la détruire. Il est donc impératif de s'assurer que Toad et les composants associés sont mis à jour régulièrement, qu'ils sont configurés correctement et qu'ils sont protégés par des contrôles de sécurité appropriés pour éliminer ces risques. Remarque : Indépendamment de l'architecture et des protocoles de sécurité en place, les composants stratégiques à maintenir à jour sont les systèmes d'exploitation et les plateformes de base de données elles-mêmes. Par extension, cela inclut également l'IDE de base de données, car toutes les vulnérabilités de sécurité présentes dans un IDE ou dans ses composants associés peuvent potentiellement compromettre la sécurité de l'ensemble de l'environnement de base de données.

SÉCURITÉ DES APPLICATIONS ET MISE À JOUR DE TOAD

Ensuite, n'oubliez pas votre rôle, qui est de mettre à jour vos logiciels continuellement pour garantir la sécurité du réseau. Les attaques par rançongiciel ayant exploité la vulnérabilité WannaCry/Petya ont montré que des centaines de milliers d'ordinateurs dans le monde exécutaient des logiciels obsolètes. (C'est probablement encore le cas de beaucoup.) Et même si le correctif associé à la vulnérabilité WannaCry a été distribué dans le cadre d'une mise à jour normale de Windows, de trop nombreuses entreprises n'ont pas pris la peine de l'appliquer. Malgré des mois d'avertissements, Petya a lancé une seconde vague d'attaques exploitant la même vulnérabilité, attaques qui ont touché les ordinateurs qui n'avaient toujours pas été mis à jour.

D'accord, certains groupes informatiques retardent les mises à jour qui forcent à redémarrer le système et qui coupent la productivité. Certains craignent l'effet de ces mises à jour sur les applications dont des milliers d'utilisateurs dépendent. D'autres ne donnent la priorité qu'aux mises à jour nécessaires, et déterminent eux-mêmes ce qui entre dans la définition de ce terme. D'autres encore suivent une approche de la mise à jour de Toad et d'autres logiciels de développement du type : tant que ce n'est pas cassé, il n'y a pas besoin de le réparer.

Vulnérabilités identifiées

Voici un exemple qui montre pourquoi les utilisateurs doivent faire attention et utiliser la dernière version prise en charge. Il y a plusieurs années, dans le cadre de ses vérifications habituelles pendant le processus de build/publication, Quest a identifié et corrigé une vulnérabilité dans Toad for Oracle 13.1.1, avec la notification suivante :

« Quest a récemment corrigé une bibliothèque [tierce], dans laquelle une vulnérabilité de niveau critique (CVSS 9.3) a été découverte. Cette vulnérabilité affectait la bibliothèque Microsoft Visual C++ et pouvait mener à une escalade des privilèges. Cette vulnérabilité a été corrigée avec la version la plus récente de Toad. »

Si en lisant ces lignes, vous vous dites : « Il fonctionne avec la version d'Oracle que je dois utiliser… alors où est le problème ? »

« Il fonctionne avec la version d'Oracle que je dois utiliser… alors où est le problème ? »

N'est-il pas extraordinaire qu'un logiciel publié il y a 10 ans fonctionne avec une base de données sortie 9 ans plus tard ? La postcompatibilité est une chose rare de nos jours.

En revanche, du point de vue de la cybersécurité, les bonnes pratiques ne sont pas respectées, indépendamment de l'architecture employée et des protocoles de sécurité ou pare-feu en place. L'utilisation de logiciels dont le support n'est plus assuré peut les rendre vulnérables aux menaces de sécurité, car ils se retrouvent sans mises à jour ni correctifs, ce qui peut compromettre l'intégrité et la confidentialité des données avec lesquelles ils interagissent. Les sources des cybermenaces se diversifient et augmentent parallèlement au recours accru à des bibliothèques open source dans les logiciels propriétaires.

En 2018, une étude de Fossa a révélé que 92 % des projets logiciels utilisaient des composants open source, et que l'application moyenne contient 57 % de code ouvert. De même, en 2019, Synopsis a découvert que le code ouvert représentait en moyenne 70 % du code des applications propriétaires analysées

Arrive 2021 et la crise Log4j. La cybermenace Log4j exploitait une vulnérabilité de la bibliothèque Apache Log4j, un outil de journalisation open source très populaire pour les applications Java. Cette vulnérabilité permettait aux pirates d'exécuter à distance du code malveillant sur les systèmes affectés, pouvant entraîner vols de données, attaques par rançongiciel et autres failles de sécurité.

La vulnérabilité Log4j a touché un grand nombre d'organisations dans le monde entier, et la vitesse et la portée de l'exploit ont soulevé des questions sur la sécurité des logiciels open source et la nécessité de mettre en place des mesures de cybersécurité plus robustes.

En résumé, sans nomenclature, impossible de réellement connaître les dépendances d'un logiciel, ni de savoir d'où surgira la prochaine menace. La seule garantie que vous avez, c'est lorsque vous utilisez un logiciel toujours pris en charge proposant des correctifs en cas de nouvelle menace.

Je répète la question. Savez-vous quelle version de Toad vous utilisez et si elle est toujours prise en charge ? Quest publie continuellement des versions plus récentes et plus sécurisées de ses logiciels. Voici un exemple. Le Tableau 1 retrace l'historique des versions de Toad for Oracle. Tous les logiciels antérieurs à la version 15.0 ne bénéficient plus d'aucun support.

Les versions plus récentes des produits Toad, comme Toad for Oracle, contiennent bien plus que des améliorations fonctionnelles : elles incluent également des améliorations conséquentes en matière de sécurité.

L'évolution des versions de Toad a suivi de près celle du paysage des menaces et vulnérabilités dans le domaine du développement de bases de données, notamment :

- Connexions non sécurisées (non chiffrées) à une base de données
- Escalade involontaire des privilèges (un utilisateur à faibles privilèges devient super utilisateur, par exemple)
- Protections anormalement faibles pour l'accès aux informations personnelles identifiables (PII) et aux données sensibles stockées dans le Cloud
- PII stockées (et oubliées) dans des copies hors production des bases de données

Au moins deux fois par an, les clients de Quest ont la possibilité de mettre Toad à jour vers la version la plus récente et d'ajouter des améliorations de sécurité qui éliminent ce type de menaces.

Versions et support de Toad for Oracle

Version	Support	Date de disponibilité générale
16.3	**Support complet**	7 avril 2023
16.2	**Support complet**	30 septembre 2022
16.1	**Support limité**	29 juin 2022
16.0	**Support limité**	26 avril 2022
15.1	**Support limité**	27 janvier 2022
15.0	**Support limité**	18 octobre 2021
14.2	**Support arrêté**	13 juillet 2021
14.1	**Support arrêté**	30 mars 2021
14.0	**Support arrêté**	23 octobre 2020

Tableau 1. Les versions de produit antérieures qui ne figurent pas dans le tableau sont considérées comme arrêtées. Reportez-vous au tableau de prise en charge des versions de Toad for Oracle pour obtenir les informations les plus récentes. (ICI)

CONTRÔLES DE SÉCURITÉ POUR EMPÊCHER LES ATTAQUES SUR LA CHAÎNE LOGISTIQUE

Avec la complexité des environnements logiciels actuels, les administrateurs informatiques doivent relever un certain nombre de défis en matière de sécurité. Ils doivent notamment gérer les vulnérabilités sur plusieurs applications et plateformes. Avec l'utilisation de plus en plus répandue des bibliothèques open source, il devient de plus en plus pressant d'identifier et de gérer les dépendances au sein de la chaîne logistique logicielle.

La gestion efficace des dépendances logicielles est essentielle pour garantir la sécurité des systèmes et éliminer les risques de cyberattaques ou de complications juridiques liées à des problèmes de licences. Pour y parvenir, les organisations doivent se concentrer en priorité sur la sécurité de la chaîne logistique et mettre en œuvre des stratégies pour la gestion et la surveillance des dépendances tout au long du cycle de développement des logiciels.

L'évolution de Toad suit de près celle du paysage des menaces et vulnérabilités dans le domaine du développement de bases de données.

Quest constate une inquiétude grandissante par rapport aux attaques de la chaîne logistique, qui introduisent des logiciels malveillants dans les produits avant leur publication auprès de la clientèle. Une série de contrôles d'analyse permet de suivre les standards de sécurité des logiciels pour identifier et éliminer les logiciels malveillants pendant le processus de build des produits Toad de Quest, notamment Toad for Oracle. Ces contrôles garantissent que les produits ne présentent ni vulnérabilité ni logiciel malveillant, qu'ils ne contiennent pas de portes dérobées et qu'ils sont développés par des collaborateurs et des sous-traitants dont le mot d'ordre est l'intégrité. Le Tableau 2 présente les contrôles de sécurité auxquels chaque version de Toad est soumise.

Contrôle de sécurité	Description
1. Formation sur la sécurité	Les développeurs, responsables et directeurs doivent suivre 2,5 heures de formation spécifique sur la sécurité.
2. Cycle de développement logiciel sécurisé	Le cycle de développement suit les bonnes pratiques du service Information and Systems Management (ISM) de Quest.
3. Correctifs logiciels tiers	Les logiciels tiers groupés sont soumis à un processus standard de recherche des vulnérabilités avant la publication de l'application.
4. Analyse de vulnérabilités	Tous les logiciels sont analysés à l'aide d'un produit SAST/DAST conforme aux standards du secteur pour identifier les vulnérabilités.
5. Test d'intrusion (tiers)	Les produits sont soumis à des tests d'intrusion annuels.
6. Analyse des logiciels malveillants	Tous les produits sont analysés avant leur publication à l'aide de deux outils anti-logiciel malveillant indépendants conformes aux standards du secteur.
7. Signature de code	Les logiciels distribués aux clients sont signés de manière chiffrée à l'aide de la clé de signature officielle de Quest pour en valider l'authenticité.
8. Intégrité des logiciels	Les sommes de contrôle des programmes d'installation des logiciels distribués sont publiées pour permettre aux clients d'en vérifier l'intégrité.
9. Conformité FIPS	Les données sensibles sont protégées au repos et en transit grâce à des algorithmes de chiffrement conformes aux standards FIPS.

Tableau 2 : Contrôles de sécurité de Toad contre les attaques de la chaîne logistique

- Menaces de sécurité logicielles
- Conception logicielle sécurisée
- Codage sécurisé
- Test de sécurité
- Vue d'ensemble de la sécurité et des risques
- Problèmes de code dans l'interaction avec le serveur client Web
- Problèmes d'interaction entre les applications/clients lourds et le serveur
- Problèmes dus à la mauvaise utilisation du chiffrement et des dispositifs de sécurité
- La sécurité dans le cycle de développement des logiciels

Voici comment Quest Software met en œuvre chaque contrôle de sécurité pour ses produits Toad :

1. FORMATION SUR LA SÉCURITÉ

Cette formation a pour objectif de développer des connaissances de base en matière de sécurité, d'adopter des pratiques de codage plus sécurisées et de renforcer l'application du cycle de développement logiciel sécurisé de Quest (voir ci-dessous). Voici les sujets de formation actuellement abordés :

- Comprendre la sécurité des logiciels
- Menaces de sécurité logicielles
- Conception logicielle sécurisée
- Codage sécurisé
- Test de sécurité
- Vue d'ensemble de la sécurité et des risques
- Problèmes de code dans l'interaction avec le serveur client Web
- Problèmes d'interaction entre les applications/clients lourds et le serveur
- Problèmes dus à la mauvaise utilisation du chiffrement et des dispositifs de sécurité
- La sécurité dans le cycle de développement des logiciels

Quest contrôle les cours suivis et en garde la trace à des fins d'utilisation lors d'audits clients. Ces enregistrements prouvent que les équipes d'ingénieurs de Quest reçoivent une formation sur les pratiques de développement sécurisées.

2. CYCLE DE DÉVELOPPEMENT LOGICIEL SÉCURISÉ (SSDLC)

Le SSDLC des produits Toad intègre des considérations de sécurité et de confidentialité dans le processus de développement du produit lui-même. Le SSDLC est conçu pour aider les ingénieurs Toad à rédiger des logiciels sécurisés, à respecter les standards de sécurité des logiciels et à maintenir des coûts d'ingénierie raisonnables. Voici les différentes composantes et phases du SSDLC :

- Définir les exigences de sécurité
- Définir les indicateurs et les rapports de conformité
- Modéliser les menaces
- Définir et utiliser les standards de chiffrement
- Gérer les risques associés à l'utilisation de composants tiers
- Établir un processus de réponse aux incidents standard

3. CORRECTIFS POUR LES LOGICIELS ET COMPOSANTS TIERS

Comme nombre de fournisseurs de logiciels d'entreprise, Quest intègre souvent du code écrit par d'autres entreprises (« tierces »), ce qui lui évite de tout rédiger de zéro. Mais avec le temps, des vulnérabilités qui requièrent un correctif apparaissent dans certains composants tiers. Outre la consultation de la base de données des CVE du NIST pour obtenir des informations sur les vulnérabilités actuelles, Quest utilise également des outils pour identifier les DLL tierces et les vulnérabilités que ces bibliothèques peuvent contenir. Quest a également développé un processus visant à réduire la probabilité de publier un logiciel intégrant des composants tiers vulnérables. Le processus :

- Définit les critères des vulnérabilités rédhibitoires.
- Requiert un inventaire de tous les composants, logiciels et DLL tiers intégrés dans les produits
- Exige des contrôles réguliers à la recherche de vulnérabilités dans les composants tiers.
- Définit des échéances (30/60/180 jours) que les tiers doivent respecter pour la correction des composants vulnérables.
- Exige que les clients soient notifiés de l'application d'un correctif aux produits et de la publication d'une nouvelle version.

4. ANALYSE DES VULNÉRABILITÉS (SAST et DAST)

Quest a défini des processus d'analyse SAST (Static Application Security Testing) et DAST (Dynamic Application Security Testing), qui utilisent des outils externes.

La méthode SAST est une forme de test en boîte blanche. Les testeurs utilisant cette méthode examinent l'application de l'intérieur, recherchant dans son code source des conditions indiquant des vulnérabilités de sécurité potentielles. La méthode DAST est une forme de test en boîte noire, de l'extérieur, du point de vue du pirate qui regarderait l'application. Les testeurs utilisant cette méthode examinent l'application Web lors de son exécution et essaient de la pirater comme un hacker le ferait.

Les outils SAST permettent d'identifier les faiblesses répertoriées dans une liste appelée Common Weakness Enumeration (CWE). Ces outils sont limités pour la gestion des problèmes de flux logique, d'authentification et d'autorisation, mieux gérés par les tests d'intrusion (voir ci-dessous) ou les examens de code source manuels. Les outils d'analyse DAST, qui interagissent avec une application Web depuis l'extérieur, s'appuient sur le protocole HTTP et ne sont rattachés à aucune technologie spécifique.

Pour les produits Toad, le processus se déroule comme suit :

- Des analyses complètes du produit/de l'application Web sont effectuées automatiquement là où cela est possible, au moins deux fois par an et avant la publication de chaque version, à l'aide de l'outil SAST/DAST approprié.
- Tout le code produit développé par Quest est analysé par l'outil SAST/DAST.
- Le responsable de la sécurité des produits Toad examine les résultats de chaque analyse, et si nécessaire, collabore avec l'ingénieur InfoSec principal pour déterminer la gravité des problèmes identifiés.
- Aucun produit n'est publié s'il contient des vulnérabilités critiques ou sérieuses.
- Si des vulnérabilités moyennes ou faibles sont identifiées, le responsable de la sécurité collabore avec l'architecte produit pour les corriger.
- Le responsable de la sécurité et l'architecte produit déterminent la solution la mieux adaptée à chaque vulnérabilité détectée par les analyses.

La méthode SAST consiste à examiner l'application de l'intérieur, recherchant dans son code source des vulnérabilités de sécurité potentielles. La méthode DAST est une forme de test en boîte noire, de l'extérieur, du point de vue du pirate qui regarderait l'application Web.

5. TEST D'INTRUSION (TIERS)

Le test d'intrusion montre l'impact concret de l'exploitation d'une vulnérabilité ou d'une faiblesse du processus. Il est conçu pour évaluer la sécurité avant une attaque éventuelle. Un test d'intrusion n'est pas une analyse automatique d'une application ou de son code source. Il s'agit plutôt de l'étape qui suit l'analyse automatisée des vulnérabilités (voir ci-dessus).

Pour les produits Toad, les tests d'intrusion sont réalisés chaque année. Ces tests, manuels et automatisés, sont conçus pour faire respecter les standards de sécurité logiciels dans les aspects suivants du produit :

- Logique d'application
- Injection de code
- Stockage local
- Exploitation binaire et rétro-ingénierie
- Privilèges excessifs
- Stockage non chiffré des informations sensibles
- Transmission non chiffrée des informations sensibles
- Mises en œuvre faibles du chiffrement
- Contrôles d'assemblage faibles
- Contrôles de l'interface graphique faibles
- Mots de passe faibles ou par défaut

Dans la plupart des cas, un test d'intrusion suit un cadre spécifique en fonction de l'application ou de l'infrastructure cible, et les tactiques varient en fonction de l'attaque simulée.

Pourquoi mettre Toad à jour

Suite à un test d'intrusion, Quest a identifié et corrigé une vulnérabilité dans Toad for Oracle 13.3 et en a averti les clients : « Lors d'un récent test d'intrusion, un problème a été détecté : l'utilisateur n'était pas notifié en cas de connexion non sécurisée à une base de données. Lorsqu'un utilisateur se connecte sans le savoir à un système via un lien non chiffré, un pirate peut capturer ses informations d'identification ou toutes les données transférées via cette connexion. Quest a corrigé cette faille. »

6. ANALYSE DES BUILDS LOGICIELS À LA RECHERCHE DE LOGICIELS MALVEILLANTS

Lorsque les builds des produits Toad sont packagés pour la publication, ils sont tout d'abord analysés à la recherche de logiciels malveillants d'après un processus cohérent :

- Les packages d'installation sont hachés à l'aide d'un algorithme SHA-256 avant l'analyse, et ce hachage doit correspondre au hachage final publié dans le package.

Tous les builds logiciels sont analysés à la recherche de logiciels malveillants avant leur publication pour installation.

- Tous les fichiers packagés dans un programme d'installation sont d'abord analysés à la recherche de logiciels malveillants.
- La recherche des logiciels malveillants est automatisée (script ou processus de ligne de commande).
- Nous utilisons des outils de recherche de logiciels malveillants indépendants (deux pour Windows et deux pour Linux), mis à jour avec les dernières signatures/ définitions avant l'analyse.
- Un enregistrement de preuve dans lequel figurent l'heure, la date et les résultats de chaque analyse est produit et conservé indéfiniment.
- Les directeurs de la sécurité et de l'ingénierie doivent approuver les exceptions pour tous les fichiers du package.

Le processus est conçu pour assurer le respect de plusieurs standards de sécurité des logiciels :

Les packages d'installation sont hachés à l'aide d'un algorithme SHA-256 avant l'analyse, et ce hachage doit correspondre au hachage final publié dans le package.

- Tous les builds logiciels sont analysés à la recherche de logiciels malveillants avant leur publication pour installation.
- Tous les fichiers packagés dans un programme d'installation sont d'abord analysés à la recherche de logiciels malveillants.
- La recherche des logiciels malveillants est automatisée (script ou processus de ligne de commande).
- Nous utilisons des outils de recherche de logiciels malveillants indépendants (deux pour Windows et deux pour Linux), mis à jour avec les dernières signatures/ définitions avant l'analyse.
- Un enregistrement de preuve dans lequel figurent l'heure, la date et les résultats de chaque analyse est produit et conservé indéfiniment.
- Les directeurs de la sécurité et de l'ingénierie doivent approuver les exceptions pour tous les fichiers du package.

7. & 8. SIGNATURE DE CODE ET INTÉGRITÉ DES LOGICIELS

Une application portant le certificat de signature de code de Quest est l'assurance pour le client que Quest a créé l'application et que le logiciel est fiable. Le processus de signature de code a pour objectif de garantir l'authenticité du logiciel en vérifiant son auteur. Il permet également de s'assurer de l'intégrité du logiciel en montrant que le code n'a pas été altéré depuis qu'il a été signé. La signature de

code joue aussi un rôle dans la publication des mises à jour et des correctifs. Lorsque Quest signe la mise à jour d'un produit Toad avec la même clé que celle de l'application d'origine, c'est un gage de fiabilité : la mise à jour n'aurait pas pu provenir d'une autre source que Quest. Enfin, les sommes de contrôle générées pendant la signature de code garantissent aux utilisateurs qu'ils ont reçu le bon fichier, et non un fichier signé à l'aide d'une clé volée. Tous les systèmes d'exploitation et navigateurs majeurs prennent en charge la signature de code pour empêcher la distribution de code malveillant.

Quest signe chaque fichier .exe et .dll du programme d'installation, ainsi que les fichiers binaires packagés avec les fichiers de l'application et du programme d'installation eux-mêmes.

9. PROTECTION DES DONNÉES SENSIBLES CONFORME AUX STANDARDS FIPS

La présence de données sensibles dans vos applications et bases de données impose une protection. Les données sensibles englobent pratiquement tous les types de données que vous ne voudriez pas voir tomber entre de mauvaises mains :

- Informations d'identification réseau
- Mots de passe
- Numéros de sécurité sociale
- Informations de carte bancaire
- Informations personnelles identifiables (PII) comme les noms, les adresses et les numéros de téléphone
- Informations personnelles sur la santé (PHI)
- Informations financières
- Dossiers internes
- Propriété intellectuelle

La famille de produits Toad protège les données sensibles grâce à des algorithmes de chiffrement conformes aux standards FIPS du gouvernement des États-Unis. De plus, elle applique cette protection aux données sensibles à la fois en transit et au repos.

Les standards FIPS définissent les bonnes pratiques et exigences relatives aux systèmes de sécurité basés sur le chiffrement, notamment concernant les méthodes de chiffrement et la génération de clés de chiffrement. La conformité aux standards FIPS est obligatoire pour tous les ordinateurs utilisés par l'administration aux États-Unis et s'étend aux tests d'applications extérieures (comme Toad) destinées à être exécutées sur les ordinateurs des administrations américaines.

Tous les produits Quest utilisent des algorithmes conformes aux standards FIPS pour le chiffrement et le hachage. Le statut de conformité FIPS actuel (actuellement FIPS 140-2) est validé avant la publication de chaque version.

Les produits Toad utilisent au moins une des bibliothèques/classes ou un des fournisseurs de services de chiffrement suivants :

- SHA-256 (.NET)
- DSA (.NET)
- RSA (.NET)
- ECDSA (.NET)
- AES (.NET)
- Java Cryptography Class

Tous les produits Quest utilisent des algorithmes conformes aux standards FIPS pour le chiffrement et le hachage. Le statut de conformité FIPS actuel (actuellement FIPS 140-2) est validé avant la publication de chaque version.

Pourquoi mettre Toad à jour

Suite au test de conformité FIPS 140-2, Quest a identifié et corrigé une vulnérabilité dans Toad for Oracle 13.2, puis en a averti les clients :

« Il a été porté à l'attention de Quest qu'un exploit actif permettait aux pirates de déchiffrer les informations d'identification enregistrées dans le produit Toad. Cette faille, qui permettait d'exploiter la méthode de chiffrement des mots de passe utilisée par Toad, pouvait être utilisée pour déchiffrer et utiliser les informations d'identification des utilisateurs et compromettre les bases de données, serveurs FTP ou serveurs SSH affectés. Depuis cette découverte, Quest a mis en œuvre un chiffrement fort, a corrigé cette vulnérabilité et a publié une version non vulnérable du logiciel. »

RESPECT DES STANDARDS DE SÉCURITÉ DES LOGICIELS

	Formation sur la sécurité	Correctifs pour les logiciels et composants tiers	Analyse de vulnérabilités	Analyse des builds logiciels à la recherche de logiciels malveillants	Signature de code et intégrité des logiciels
NIST SP 800-53 R4	✓	✓	✓	✓	✓
ISO 27001	✓	✓	✓	✓	
PCI DSS v3.0	✓	✓	✓		
PCI 1.4				✓	
AICPA TSC 2014		✓	✓		
AICPA TSC (SOC-2)				✓	
HIPAA 45 C.F.R.		✓	✓	✓	

CONCLUSION

Les contrôles de sécurité décrits ci-dessus sont conçus et appliqués pour éliminer les risques de sécurité sur la chaîne logistique des produits Toad. La Figure 2 en illustre le flux.

Les produits Toad sont appréciés et plébiscités, et ils ont fait gagner des millions d'heures de productivité aux professionnels des bases de données. En mettant à jour les produits Toad, vous assurez un flux continu de nouvelles fonctionnalités et le respect des standards de sécurité des logiciels. Vous bénéficiez d'un support technique complet et vous maintenez un profil de sécurité à toute épreuve dans votre organisation.

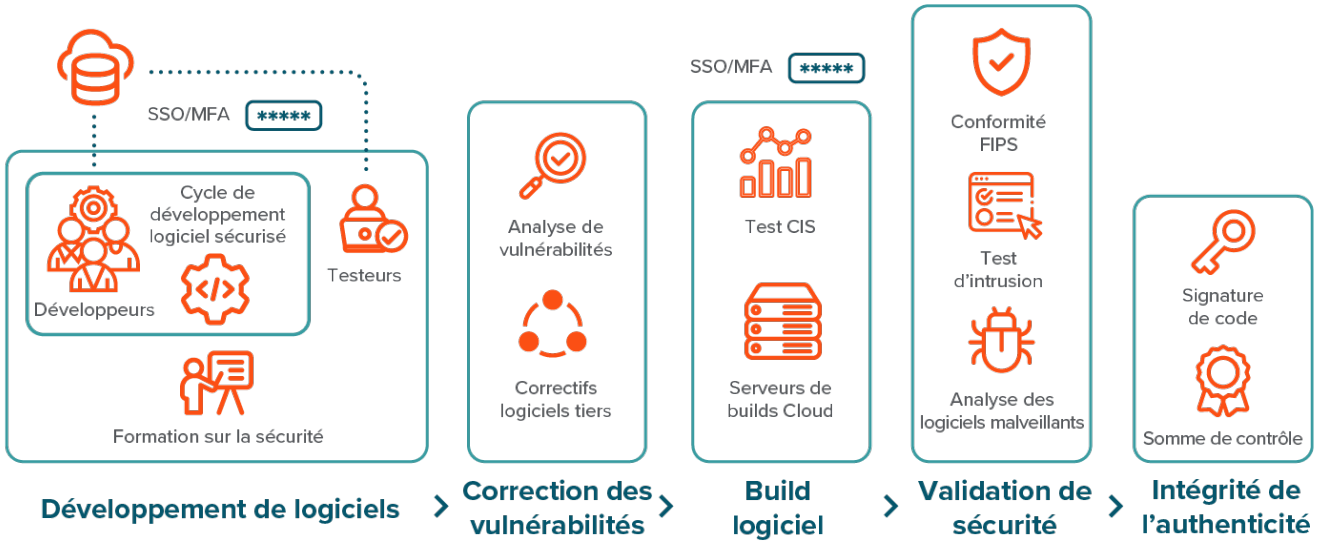

Figure 2 : Flux des contrôles de sécurité dans le cycle de développement des produits Toad

À PROPOS DES AUTEURS

Julie Hyman est cheffe de produit senior chargée du portefeuille d'outils de base de données chez Quest Software. Cette cheffe de produit logiciel chevronnée cumule 25 ans d'expérience dans la création et l'amélioration de solutions logicielles dans des start-ups et des firmes figurant au classement Fortune 500. Depuis de nombreuses années, Julie collabore étroitement avec des administrateurs de base de données, des développeurs et des analystes issus de différents secteurs et de sociétés majeures afin de garantir que Quest propose toujours des solutions de classe mondiale.

Ryan Crochet est responsable marketing produit senior dans la division Information and Systems Management de Quest Software. Passionné par le marché qu'il couvre et les problèmes qu'il y rencontre régulièrement, Ryan cherche continuellement à les résoudre tout en mettant en avant la puissance de la prise de décision basée sur les données pour aligner l'expertise technique et les résultats commerciaux.

À propos de Quest

Quest crée des solutions logicielles qui exploitent les avantages des nouvelles technologies dans un paysage informatique toujours plus complexe. De la gestion des bases de données et des systèmes à la migration et à la gestion d'Active Directory et de Microsoft 365, en passant par la cyberrésilience, Quest aide ses clients à relever leurs prochains défis informatiques dès à présent. Partout dans le monde, plus de 130 000 entreprises et 95 % de celles du classement Fortune 500 font confiance à Quest pour assurer une gestion et une surveillance proactives afin de soutenir toute nouvelle initiative, de surmonter les défis Microsoft complexes et de garder une longueur d'avance sur les menaces à venir. Quest Software. Où demain rencontre aujourd'hui. Pour en savoir plus, consultez le site quest.com.

Brevets

Chez Quest Software, nous sommes fiers de notre technologie de pointe. Des brevets ou des brevets en attente peuvent s'appliquer à ce produit. Pour obtenir des informations récentes sur les brevets applicables à ce produit, consultez notre site Web à l'adresse suivante : www.quest.com/legal.

Marques

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

www.quest.com/fr-fr/company/contact-us.aspx