Sécurité des produits

Enterprise applications

NetApp
May 03, 2024

Sommaire

Sécurité des produits

Les outils ONTAP pour VMware vSphere

L'ingénierie logicielle avec les outils ONTAP pour VMware vSphere utilise les activités de développement sécurisé suivantes :

- **Modélisation des menaces.** le but de la modélisation des menaces est de découvrir des défauts de sécurité dans une fonction, un composant ou un produit au début du cycle de vie du développement logiciel. Un modèle de menace est une représentation structurée de toutes les informations qui affectent la sécurité d'une application. En substance, c'est une vision de l'application et de son environnement par le biais du principe de sécurité.
- **Dynamic application Security Testing (DAST).** cette technologie est conçue pour détecter les conditions vulnérables sur les applications dans leur état d'exécution. DAST teste les interfaces HTTP et HTML exposées des applications Web-enable.
- **Devise de code tierce.** dans le cadre du développement de logiciels avec des logiciels open-source (OSS), vous devez corriger les vulnérabilités de sécurité qui pourraient être associées à tout OSS intégré à votre produit. Il s'agit d'un effort continu car une nouvelle version OSS peut avoir une nouvelle vulnérabilité découverte signalée à tout moment.
- **Analyse des vulnérabilités** l'analyse des vulnérabilités a pour but de détecter les vulnérabilités de sécurité courantes et connues dans les produits NetApp avant leur publication auprès des clients.
- * Tests de pénétration.* le test de pénétration est le processus d'évaluation d'un système, d'une application Web ou d'un réseau pour trouver des vulnérabilités de sécurité qui pourraient être exploitées par un attaquant. Les tests d'intrusion chez NetApp sont réalisés par un groupe d'entreprises tierces de confiance et approuvées. Leur domaine de test comprend le lancement d'attaques contre une application ou un logiciel similaire à des intrus hostiles ou des pirates informatiques à l'aide de méthodes ou d'outils d'exploitation sophistiqués.

Fonctionnalités de sécurité du produit

Les outils ONTAP pour VMware vSphere comprennent les fonctions de sécurité suivantes dans chaque version.

- **Bannière de connexion.** SSH est désactivé par défaut et n'autorise que les connexions à une seule fois si elles sont activées à partir de la console VM. La bannière de connexion suivante s'affiche une fois que l'utilisateur a saisi un nom d'utilisateur dans l'invite de connexion :

  AVERTISSEMENT: l'accès non autorisé à ce système est interdit et sera poursuivi par la loi. En accédant à ce système, vous convenez que vos actions peuvent être surveillées si vous soupçonnez une utilisation non autorisée.

  Une fois la connexion établie par l'utilisateur via le canal SSH, le texte suivant s'affiche :

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Contrôle d'accès basé sur les rôles (RBAC).** deux types de contrôles RBAC sont associés aux outils ONTAP :
  - Privilèges de serveur vCenter natif
  - Privilèges spécifiques au plug-in vCenter. Pour plus de détails, voir "ce lien".
- **Canaux de communication cryptés.** toutes les communications externes se produisent sur HTTPS en utilisant la version 1.2 de TLS.
- **Exposition minimale au port.** seuls les ports nécessaires sont ouverts sur le pare-feu.

  Le tableau suivant décrit les détails du port ouvert.

N° de port TCP v4/v6	Direction	Fonction
8143	entrant	Connexions HTTPS pour l'API REST
8043	entrant	Connexions HTTPS
9060	entrant	Connexions HTTPS Utilisé pour les connexions SOAP sur https Ce port doit être ouvert pour permettre à un client de se connecter au serveur d'API des outils ONTAP.
22	entrant	SSH (désactivé par défaut)
9080	entrant	Connexions HTTPS - VP et SRA - connexions internes à partir du bouclage uniquement
9083	entrant	Connexions HTTPS - VP et SRA Utilisé pour les connexions SOAP sur https
1162	entrant	Paquets de déroutement SNMP VP
1527	diffusion interne uniquement	Port de base de données Derby, uniquement entre cet ordinateur et lui-même, connexions externes non acceptées — connexions internes uniquement
443	bidirectionnel	Utilisé pour les connexions aux clusters ONTAP

- **Prise en charge des certificats signés de l'autorité de certification (CA).** les outils ONTAP pour VMware vSphere prennent en charge les certificats signés de l'autorité de certification. Voir ceci "article de la base de connaissances" pour en savoir plus.
- **Audit Logging.** les offres de support peuvent être téléchargées et sont extrêmement détaillées. Les outils ONTAP consigne toutes les activités de connexion et de déconnexion de l'utilisateur dans un fichier journal distinct. Les appels d'API VASA sont connectés à un journal d'audit VASA dédié (local cxf.log).
- **Stratégies de mot de passe.** les stratégies de mot de passe suivantes sont respectées :
  - Les mots de passe ne sont pas enregistrés dans des fichiers journaux.
  - Les mots de passe ne sont pas communiqués en texte brut.
  - Les mots de passe sont configurés lors du processus d'installation lui-même.
  - L'historique des mots de passe est un paramètre configurable.
  - L'âge minimum du mot de passe est défini sur 24 heures.
  - La saisie automatique des champs de mot de passe est désactivée.
  - Les outils ONTAP crypte toutes les informations d'identification stockées à l'aide de la fonction de hachage SHA256.

Plug-in SnapCenter VMware vSphere

Le plug-in NetApp SnapCenter pour l'ingénierie logicielle VMware vSphere exploite les activités de développement sécurisées suivantes :

- **Modélisation des menaces.** le but de la modélisation des menaces est de découvrir des défauts de sécurité dans une fonction, un composant ou un produit au début du cycle de vie du développement logiciel. Un modèle de menace est une représentation structurée de toutes les informations qui affectent la sécurité d'une application. En substance, c'est une vision de l'application et de son environnement par le biais du principe de sécurité.
- **Test dynamique de sécurité des applications (DAST).** technologies conçues pour détecter les conditions vulnérables des applications dans leur état d'exécution. DAST teste les interfaces HTTP et HTML exposées des applications Web-enable.
- **Devise de code tierce.** dans le cadre du développement de logiciels et de l'utilisation de logiciels open-source (OSS), il est important de traiter les vulnérabilités de sécurité qui pourraient être associées à OSS qui a été intégré à votre produit. Il s'agit d'un effort continu car la version du composant OSS peut avoir une vulnérabilité nouvellement découverte signalée à tout moment.
- **Analyse des vulnérabilités** l'analyse des vulnérabilités a pour but de détecter les vulnérabilités de sécurité courantes et connues dans les produits NetApp avant leur publication auprès des clients.
- * Tests de pénétration.* le test de pénétration est le processus d'évaluation d'un système, d'une application Web ou d'un réseau pour trouver des vulnérabilités de sécurité qui pourraient être exploitées par un attaquant. Les tests d'intrusion chez NetApp sont réalisés par un groupe d'entreprises tierces de confiance et approuvées. Leur domaine de test comprend le lancement d'attaques contre une application ou un logiciel comme des intrus hostiles ou des pirates informatiques à l'aide de méthodes ou d'outils d'exploitation sophistiqués.
- **Activité de réponse aux incidents de sécurité des produits.** les vulnérabilités de sécurité sont découvertes à la fois en interne et en externe dans l'entreprise et peuvent constituer un risque sérieux pour la réputation de NetApp si elles ne sont pas traitées dans les délais impartis. Pour faciliter ce processus, l'équipe d'intervention en cas d'incident de sécurité des produits (PSIRT) signale et effectue le suivi des vulnérabilités.

Fonctionnalités de sécurité du produit

Le plug-in NetApp SnapCenter pour VMware vSphere inclut les fonctionnalités de sécurité suivantes dans chaque version :

- **Accès limité au shell.** SSH est désactivé par défaut, et les connexions à une seule fois ne sont autorisées que si elles sont activées à partir de la console VM.
- **Avertissement d'accès dans la bannière de connexion.** la bannière de connexion suivante s'affiche après que l'utilisateur ait entré un nom d'utilisateur dans l'invite de connexion :

  AVERTISSEMENT: l'accès non autorisé à ce système est interdit et sera poursuivi par la loi. En accédant à ce système, vous convenez que vos actions peuvent être surveillées si vous soupçonnez une utilisation non autorisée.

  Une fois que l'utilisateur a terminé sa connexion via le canal SSH, les valeurs de sortie suivantes s'affichent :

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Contrôle d'accès basé sur les rôles (RBAC).** deux types de contrôles RBAC sont associés aux outils ONTAP :
  - Privilèges de serveur vCenter natif.
  - Privilèges spécifiques au plug-in VMware vCenter. Pour plus d'informations, voir "Contrôle d'accès basé sur des rôles (RBAC)".
- **Canaux de communication cryptés.** toutes les communications externes sont effectuées via HTTPS en utilisant TLS.
- **Exposition minimale au port.** seuls les ports nécessaires sont ouverts sur le pare-feu.

Le tableau suivant fournit les détails du port ouvert.

Numéro de port TCP v4/v6	Fonction
8144	Connexions HTTPS pour l'API REST
8080	Connexions HTTPS pour interface graphique OVA
22	SSH (désactivé par défaut)
3306	MySQL (connexions internes uniquement, connexions externes désactivées par défaut)
443	Nginx (services de protection des données)

- **Prise en charge des certificats signés par l'autorité de certification (CA).** le plug-in SnapCenter pour VMware vSphere prend en charge la fonctionnalité des certificats signés par l'autorité de certification. Voir "Comment créer et/ou importer un certificat SSL dans le plug-in SnapCenter pour VMware vSphere

(SCV)".

- **Stratégies de mot de passe.** les stratégies de mot de passe suivantes sont en vigueur :
  - Les mots de passe ne sont pas enregistrés dans des fichiers journaux.
  - Les mots de passe ne sont pas communiqués en texte brut.
  - Les mots de passe sont configurés lors du processus d'installation lui-même.
  - Toutes les informations d'identification sont stockées à l'aide d'un hachage SHA256.
- **Image du système d'exploitation de base.** le produit est fourni avec le système d'exploitation de base Debian pour OVA avec accès restreint et accès au shell désactivé. Cela réduit l'empreinte d'attaque. Chaque système d'exploitation de base SnapCenter est mis à jour avec les derniers correctifs de sécurité disponibles pour une protection maximale.

NetApp développe des fonctionnalités logicielles et des correctifs de sécurité en ce qui concerne le plug-in SnapCenter pour l'appliance VMware vSphere, puis les publie auprès de ses clients sous la forme d'un pack logiciel. Étant donné que ces dispositifs intègrent des dépendances spécifiques au système d'exploitation Linux et à notre logiciel propriétaire, NetApp vous recommande de ne pas modifier le système sous-exploitation, car il présente un potentiel important d'affecter l'appliance NetApp. Cela pourrait affecter la capacité de NetApp à prendre en charge l'appliance. NetApp recommande de tester et de déployer la dernière version de code pour les appliances, car elles sont publiées pour corriger les problèmes de sécurité.

Informations sur le copyright

Informations sur les marques commerciales