製品のセキュリティ
Enterprise applications

NetApp
May 03, 2024

目次

製品のセキュリティ

VMware vSphere 用の ONTAP ツール

ONTAP Tools for VMware vSphereを使用したソフトウェアエンジニアリングでは、次のセキュアな開発アクティビティを採用しています。

- * 脅威モデリング。 * 脅威モデリングの目的は、ソフトウェア開発ライフサイクルの早い段階で、機能、コンポーネント、または製品のセキュリティ上の欠陥を発見することです。脅威モデルとは、アプリケーションのセキュリティに影響するすべての情報を構造化したものです。本質的に、これはセキュリティの観点から見たアプリケーションとその環境です。
- * Dynamic Application Security Testing （ DAST ）。 * このテクノロジーは、実行中のアプリケーションで脆弱な状態を検出するように設計されています。DAST は、 Web 対応アプリケーションの公開 HTTP および HTML インターフェイスをテストします。
- * サードパーティーのコード通貨。 * オープンソース・ソフトウェア（ OSS ）を使用したソフトウェア開発の一環として、製品に組み込まれた OSS に関連するセキュリティ上の脆弱性に対処する必要があります。これは継続的な取り組みです。新しい OSS バージョンには、いつでも新たに検出された脆弱性が報告される可能性があります。
- * 脆弱性スキャン。 * 脆弱性スキャンは、お客様にリリースされる前にネットアップ製品の一般的なセキュリティの脆弱性と既知のセキュリティの脆弱性を検出するためのものです。
- * ペネトレーションテスト。 * ペネトレーションテストは、システム、 Web アプリケーション、またはネットワークを評価して、攻撃者によって悪用される可能性のあるセキュリティの脆弱性を検出するプロセスです。ネットアップでのペネトレーションテスト（ペンテスト）は、承認された信頼できる第三者企業のグループが実施します。テスト範囲には、高度な攻撃方法やツールを使用した悪意のある侵入者やハッカーと同様のアプリケーションまたはソフトウェアに対する攻撃の開始が含まれます。

製品のセキュリティ機能

ONTAP Tools for VMware vSphereの各リリースには、次のセキュリティ機能が含まれています。

- * ログインバナー。 * SSH はデフォルトでは無効になっており、 VM コンソールから有効になっている場合は 1 回限りのログインしか許可されません。ユーザがログインプロンプトでユーザ名を入力すると、次のログインバナーが表示されます。
- 警告： * このシステムへの不正アクセスは禁止されており、法律で訴追されます。このシステムにアクセスすることで、不正な使用が疑われる場合に、ユーザーのアクションが監視される可能性があることに同意したものとみなされます。

  ユーザがSSHチャネルを介したログインを完了すると、次のテキストが表示されます。

```
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.
```

- * ロールベースアクセス制御 (RBAC) 。 * ONTAP ツールには、次の 2 種類の RBAC 制御が関連付けられています。
  - vCenter Server 標準の権限
  - vCenter プラグインに固有の権限。詳細については、を参照してください "リンクをクリックしてください"。
- * 暗号化された通信チャネル。 * すべての外部通信は、バージョン 1.2 の TLS を使用して HTTPS 経由で行われます。
- * 最小限のポート露出。 * 必要なポートのみがファイアウォールで開かれています。

  次の表に、オープンポートの詳細を示します。

TCP v4 / V6 ポート番号	方向（ **Direction** ）	機能
8143	インバウンド	REST API 用の HTTPS 接続
8043	インバウンド	HTTPS 接続
9060	インバウンド	HTTPS 接続 SOAP over https 接続に使用されます クライアントがONTAP tools APIサーバに接続できるようにするには、このポートを開く必要があります。
22	インバウンド	SSH （デフォルトでは無効）
9080	インバウンド	HTTPS 接続 - VP および SRA - ループバックからの内部接続のみ
9083年だ	インバウンド	HTTPS 接続 - VP および SRA SOAP over https 接続に使用されます
一一六二	インバウンド	VP SNMP トラップパケット
1527年	内部のみ	Derby データベースポート。このコンピュータとそれ自体の間のみ、外部接続は許可されません — 内部接続のみ
443	双方向	ONTAP クラスタへの接続に使用します

- * 認証局（ CA ）署名証明書のサポート。 * VMware vSphere 用の ONTAP ツールは CA 署名証明書をサポートしています。を参照してください "こちらの技術情報アーティクル" を参照してください。
- * 監査ログ。 * サポートバンドルはダウンロード可能で、非常に詳細です。ONTAP ツールは、すべてのユーザログインおよびログアウトアクティビティを個別のログファイルに記録します。VASA API 呼び出しは、専用の VASA 監査ログ（ローカルの cxf.log ）に記録されます。
- * パスワードポリシー。 * 次のパスワードポリシーが適用されます。
  - パスワードはどのログファイルにも記録されません。
  - パスワードはプレーンテキストで伝達されません。

- パスワードは、インストールプロセスで設定します。
- パスワード履歴は設定可能なパラメータです。
- パスワードの最小有効期間は 24 時間に設定されます。
- パスワードフィールドの自動入力は無効です。
- ONTAP ツールは、保存されているすべてのクレデンシャル情報を SHA256 ハッシュで暗号化し

SnapCenterプラグインVMware vSphere

NetApp SnapCenter Plug-in for VMware vSphereのソフトウェアエンジニアリングでは、次のような安全な開発作業を行います。

- * 脅威モデリング。 * 脅威モデリングの目的は、ソフトウェア開発ライフサイクルの早い段階で、機能、コンポーネント、または製品のセキュリティ上の欠陥を発見することです。脅威モデルとは、アプリケーションのセキュリティに影響するすべての情報を構造化したものです。本質的に、これはセキュリティの観点から見たアプリケーションとその環境です。
- *動的アプリケーションセキュリティテスト(DAST)。*実行中のアプリケーションの脆弱な状態を検出するように設計されたテクノロジ。DAST は、 Web 対応アプリケーションの公開 HTTP および HTML インターフェイスをテストします。
- *サードパーティのコード通貨。*ソフトウェアの開発およびオープンソースソフトウェア（OSS）の使用の一環として、製品に組み込まれているOSSに関連するセキュリティの脆弱性に対処することが重要です。これは、OSSコンポーネントのバージョンに、いつでも新たに検出された脆弱性が報告される可能性があるため、継続的な取り組みです。
- * 脆弱性スキャン。 * 脆弱性スキャンは、お客様にリリースされる前にネットアップ製品の一般的なセキュリティの脆弱性と既知のセキュリティの脆弱性を検出するためのものです。
- *ペネトレーションテスト。*ペネトレーションテストは、システム、Webアプリケーション、またはネットワークを評価して、攻撃者によって悪用される可能性のあるセキュリティの脆弱性を検出するプロセスです。ネットアップでのペネトレーションテスト（ペンテスト）は、承認された信頼できる第三者企業のグループが実施します。このテスト範囲には、高度な攻撃方法やツールを使用した悪意のある侵入者やハッカーなどのアプリケーションやソフトウェアに対する攻撃の開始が含まれます。
- *製品セキュリティインシデント対応アクティビティ。*セキュリティの脆弱性は社内外で発見され、タイムリーに対処しなければ、ネットアップの評判に深刻なリスクをもたらす可能性があります。このプロセスを容易にするために、Product Security Incident Response Team（PSIRT）は脆弱性を報告して追跡します。

製品のセキュリティ機能

NetApp SnapCenter Plug-in for VMware vSphereの各リリースには、次のセキュリティ機能が含まれています。

- 制限付きシェルアクセス。 SSHはデフォルトで無効になっており、1回限りのログインはVMコンソールから有効にした場合にのみ許可されます。
- *ログインバナーのアクセス警告*ログインプロンプトにユーザ名を入力すると、次のログインバナーが表示されます。
- 警告： * このシステムへの不正アクセスは禁止されており、法律で訴追されます。このシステムにアクセスすることで、不正な使用が疑われる場合に、ユーザーのアクションが監視される可能性があることに同意したものとみなされます。

ユーザがSSHチャネルを介したログインを完了すると、次の出力が表示されます。

```
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.
```

- * ロールベースアクセス制御 (RBAC) 。 * ONTAP ツールには、次の 2 種類の RBAC 制御が関連付けられています。
  - vCenter Server標準の権限。
  - VMware vCenterプラグインに固有の権限。詳細については、を参照してください "ロールベースアクセス制御（ RBAC ）"。
- *暗号化された通信チャネル。*すべての外部通信は、TLSを使用してHTTPS経由で行われます。
- * 最小限のポート露出。 * 必要なポートのみがファイアウォールで開かれています。

次の表に、オープンポートの詳細を示します。

TCP v4 / V6ポート番号	機能
8144	REST API 用の HTTPS 接続
8080 です	OVA GUIでのHTTPS接続
22	SSH（デフォルトでは無効）
3306	mysql（内部接続のみ。外部接続はデフォルトで無効）
443	nginx（データ保護サービス）

- 認証局（**CA**）署名証明書のサポート。 SnapCenter Plug-in for VMware vSphereは、CA署名証明書の機能をサポートしています。を参照してください "SnapCenter Plug-in for VMware vSphere（SCV）にSSL証明書を作成/インポートする方法"。
- *パスワードポリシー。*次のパスワードポリシーが有効です。
  - パスワードはどのログファイルにも記録されません。
  - パスワードはプレーンテキストで伝達されません。
  - パスワードは、インストールプロセスで設定します。
  - クレデンシャル情報はすべてSHA256ハッシュを使用して保存されます。
- *基本オペレーティングシステムイメージ。*この製品は、アクセス制限とシェルアクセスが無効になったOVA用のDebianベースOSに同梱されています。これにより、攻撃のフットプリントが削減されます。すべてのSnapCenter リリースベースのオペレーティングシステムには、最大限のセキュリティを適用できる最新のセキュリティパッチが適用されています。

ネットアップでは、SnapCenter Plug-in for VMware vSphereアプライアンスに関連するソフトウェア機能およびセキュリティパッチを開発し、その後、バンドルソフトウェアプラットフォームとしてお客様にリリース

します。ネットアップでは、これらのアプライアンスにはLinuxのサブシステムに固有の依存関係と独自のソフトウェアが含まれているため、サブオペレーティングシステムを変更しないことを推奨します。これは、ネットアップアプライアンスに影響を及ぼす可能性が高いためです。これは、ネットアップがアプライアンスをサポートできるかどうかに影響します。アプライアンスはセキュリティ関連の問題にパッチを適用するためにリリースされているため、最新のコードバージョンをテストして導入することを推奨します。

著作権に関する情報

商標に関する情報