Produktsicherheit

Enterprise applications

NetApp
May 09, 2024

Inhalt

Produktsicherheit

ONTAP Tools für VMware vSphere

Das Software Engineering mit ONTAP Tools für VMware vSphere nutzt die folgenden sicheren Entwicklungsaktivitäten:

- **Threat Modeling.** der Zweck der Bedrohungsmodellierung ist es, Sicherheitslücken in einem Feature, einer Komponente oder einem Produkt frühzeitig im Lebenszyklus der Softwareentwicklung zu entdecken. Ein Bedrohungsmodell ist eine strukturierte Darstellung aller Informationen, die die Sicherheit einer Anwendung beeinflussen. Im Wesentlichen ist es ein Blick auf die Anwendung und ihre Umgebung durch die Linsen der Sicherheit.
- **Dynamic Application Security Testing (DAST).** Diese Technologie wurde entwickelt, um gefährdete Bedingungen für Anwendungen im laufenden Zustand zu erkennen. DAST testet die freigesetzten HTTP- und HTML-Schnittstellen von Web-enable-Anwendungen.
- **Codewährung von Drittanbietern.** im Rahmen der Softwareentwicklung mit Open-Source-Software (OSS) müssen Sie Sicherheitslücken schließen, die mit jedem OSS in Ihr Produkt integriert werden könnten. Dies ist ein fortdauernde Bemühung, da bei einer neuen OSS-Version möglicherweise jederzeit eine neu entdeckte Sicherheitsanfälligkeit gemeldet wird.
- **Schwachstellenscans.** Zweck der Schwachstellenanalyse ist es, häufige und bekannte Sicherheitslücken in NetApp Produkten zu erkennen, bevor diese bei den Kunden freigegeben werden.
- **Penetrationstest.** Penetrationstest ist der Prozess, um ein System, eine Web-Anwendung oder ein Netzwerk zu bewerten, um Sicherheitslücken zu finden, die von einem Angreifer ausgenutzt werden könnten. Penetrationstests (Penetrationstests) bei NetApp werden von einer Gruppe genehmigter und vertrauenswürdiger Drittanbieter durchgeführt. Ihr Testumfang umfasst die Einleitung von Angriffen gegen eine Anwendung oder Software ähnlich wie feindliche Eindringlinge oder Hacker mit ausgereiften Methoden oder Tools zur Ausbeutung.

Produktsicherheitsfunktionen

Die ONTAP Tools für VMware vSphere beinhalten in jeder Version die folgenden Sicherheitsfunktionen.

- **Anmeldebanner** SSH ist standardmäßig deaktiviert und erlaubt nur einmalige Anmeldungen, wenn sie über die VM-Konsole aktiviert sind. Das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen Benutzernamen in die Anmeldeaufforderung eingegeben hat:

  WARNUNG: der unerlaubte Zugriff auf dieses System ist verboten und wird gesetzlich verfolgt. Durch den Zugriff auf dieses System erklären Sie sich damit einverstanden, dass Ihre Maßnahmen überwacht werden können, wenn eine unbefugte Nutzung vermutet wird.

  Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird der folgende Text angezeigt:

```
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.
```

- **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC).** ONTAP Tools verfügen über zwei Arten von RBAC-Steuerungsoptionen:
  - Native vCenter Server-Berechtigungen
  - Spezifische Berechtigungen für vCenter Plug-in Weitere Informationen finden Sie unter "Dieser Link".
- **Verschlüsselte Kommunikationskanäle.** Alle externen Kommunikation erfolgt über HTTPS mit Version 1.2 von TLS.
- **Minimal Port Exposure.** nur die benötigten Ports sind an der Firewall geöffnet.

  In der folgenden Tabelle werden die Details zum offenen Anschluss beschrieben.

TCP v4/v6-Port #	Richtung	Funktion
8143	Eingehend	HTTPS-Verbindungen für REST-API
8043	Eingehend	HTTPS-Verbindungen
9060	Eingehend	HTTPS-Verbindungen Wird für SOAP-über-https-Verbindungen verwendet Dieser Port muss geöffnet werden, damit ein Client eine Verbindung zum ONTAP Tools API-Server herstellen kann.
22	Eingehend	SSH (standardmäßig deaktiviert)
9080	Eingehend	HTTPS-Verbindungen - VP und SRA - nur interne Verbindungen von Loopback
9083	Eingehend	HTTPS-Verbindungen – VP und SRA Wird für SOAP-über-https-Verbindungen verwendet
1162	Eingehend	VP SNMP-Trap-Pakete
1527	Nur zur internen Nutzung	Derby-Datenbank-Port, nur zwischen diesem Computer und sich selbst, externe Verbindungen nicht akzeptiert — nur interne Verbindungen

TCP v4/v6-Port #	Richtung	Funktion
443	Bidirektional	Wird für Verbindungen zu ONTAP-Clustern verwendet

- **Unterstützung für Zertifizierungsstelle (CA) signierte Zertifikate.** ONTAP Tools für VMware vSphere unterstützt CA signierte Zertifikate. Siehe das "kb-Artikel" Finden Sie weitere Informationen.
- **Audit Logging.** Supportpakete können heruntergeladen werden und sind äußerst detailliert. Die ONTAP Tools protokollieren alle Benutzer-Login- und -Abmeldeaktivitäten in einer separaten Protokolldatei. VASA API-Aufrufe werden in einem dedizierten VASA Audit Log (Local cxf.log) protokolliert.
- **Passwortrichtlinien.** folgende Kennwortrichtlinien werden befolgt:
  - Passwörter werden nicht in Protokolldateien protokolliert.
  - Passwörter werden nicht im Klartext kommuniziert.
  - Während des Installationsvorgangs selbst werden Passwörter konfiguriert.
  - Der Passwortverlauf ist ein konfigurierbarer Parameter.
  - Das Mindestalter des Kennworts ist auf 24 Stunden festgelegt.
  - Die Felder für das Kennwort werden automatisch ausgefüllt.
  - ONTAP-Tools verschlüsselt alle gespeicherten Anmeldeinformationen mithilfe von SHA256 Hashing.

SnapCenter Plug-in VMware vSphere

Das NetApp SnapCenter Plug-in für VMware vSphere nutzt folgende sichere Entwicklungsaktivitäten:

- **Threat Modeling.** der Zweck der Bedrohungsmodellierung ist es, Sicherheitslücken in einem Feature, einer Komponente oder einem Produkt frühzeitig im Lebenszyklus der Softwareentwicklung zu entdecken. Ein Bedrohungsmodell ist eine strukturierte Darstellung aller Informationen, die die Sicherheit einer Anwendung beeinflussen. Im Wesentlichen ist es ein Blick auf die Anwendung und ihre Umgebung durch die Linsen der Sicherheit.
- **Dynamic Application Security Testing (DAST).** Technologien, die entwickelt wurden, um gefährdete Bedingungen für Anwendungen in ihrem laufenden Zustand zu erkennen. DAST testet die freigesetzten HTTP- und HTML-Schnittstellen von Web-enable-Anwendungen.
- **Codewährung von Drittanbietern.** im Rahmen der Entwicklung von Software und der Verwendung von Open-Source-Software (OSS) ist es wichtig, Sicherheitslücken zu beheben, die mit OSS verbunden sein könnten, die in Ihr Produkt integriert wurden. Dies ist ein kontinuierlicher Aufwand, da bei der Version der OSS-Komponente eine neu entdeckte Sicherheitsanfälligkeit jederzeit gemeldet wird.
- **Schwachstellenscans.** Zweck der Schwachstellenanalyse ist es, häufige und bekannte Sicherheitslücken in NetApp Produkten zu erkennen, bevor diese bei den Kunden freigegeben werden.
- **Penetrationstest.** Penetrationstest ist der Prozess, um ein System, eine Web-Anwendung oder ein Netzwerk zu evaluieren, um Sicherheitslücken zu finden, die von einem Angreifer ausgenutzt werden könnten. Penetrationstests (Penetrationstests) bei NetApp werden von einer Gruppe genehmigter und vertrauenswürdiger Drittanbieter durchgeführt. Ihr Testumfang umfasst die Einleitung von Angriffen gegen eine Anwendung oder Software wie feindliche Eindringlinge oder Hacker mit ausgereiften Exploitationsmethoden oder -Tools.
- **Aktion zur Reaktion auf Produktsicherheitsvorfälle.** Sicherheitsschwachstellen werden sowohl intern als auch extern im Unternehmen entdeckt und können ein ernsthaftes Risiko für den Ruf von NetApp darstellen, wenn sie nicht rechtzeitig behoben werden. Zur Erleichterung dieses Prozesses meldet ein

PSIRT (Product Security Incident Response Team) die Sicherheitsanfälligkeiten und verfolgt diese.

Produktsicherheitsfunktionen

Das NetApp SnapCenter Plug-in für VMware vSphere umfasst die folgenden Sicherheitsfunktionen in jeder Version:

- **Eingeschränkter Shell-Zugriff.** SSH ist standardmäßig deaktiviert, und einmalige Anmeldungen sind nur erlaubt, wenn sie über die VM-Konsole aktiviert sind.
- **Zugangswarnung im Anmeldebanner.** das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen Benutzernamen in die Anmeldeaufforderung eingegeben hat:

  WARNUNG: der unerlaubte Zugriff auf dieses System ist verboten und wird gesetzlich verfolgt. Durch den Zugriff auf dieses System erklären Sie sich damit einverstanden, dass Ihre Maßnahmen überwacht werden können, wenn eine unbefugte Nutzung vermutet wird.

  Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird die folgende Ausgabe angezeigt:

```
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.
```

- **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC).** ONTAP Tools verfügen über zwei Arten von RBAC-Steuerungsoptionen:
  - Native vCenter Server-Berechtigungen.
  - Spezifische Berechtigungen für VMware vCenter Plug-in Weitere Informationen finden Sie unter "Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)".
- **Verschlüsselte Kommunikationskanäle.** Alle externen Kommunikation erfolgt über HTTPS mit TLS.
- **Minimal Port Exposure.** nur die benötigten Ports sind an der Firewall geöffnet.

Die folgende Tabelle enthält die Details zum offenen Anschluss.

TCP v4/v6-Portnummer	Funktion
8144	HTTPS-Verbindungen für REST-API
8080	HTTPS-Verbindungen für OVA GUI
22	SSH (standardmäßig deaktiviert)
3306	MySQL (nur interne Verbindungen; externe Verbindungen standardmäßig deaktiviert)
443	Nginx (Datensicherungsservices)

- **Unterstützung für Zertifizierungsstelle (CA) signierte Zertifikate.** SnapCenter Plug-in für VMware vSphere unterstützt die Funktion von CA signierten Zertifikaten. Siehe "Erstellen und/oder Importieren

eines SSL-Zertifikats in das SnapCenter Plug-in für VMware vSphere (SCV)".

- **Passwortrichtlinien.** die folgenden Kennwortrichtlinien sind in Kraft:
  - Passwörter werden nicht in Protokolldateien protokolliert.
  - Passwörter werden nicht im Klartext kommuniziert.
  - Während des Installationsvorgangs selbst werden Passwörter konfiguriert.
  - Alle Anmeldeinformationen werden mit SHA256 Hashing gespeichert.
- **Basis Betriebssystem-Image.** das Produkt wird mit Debian Base OS für OVA ausgeliefert, mit eingeschränktem Zugriff und Shell-Zugriff. So wird die Angriffsfläche reduziert. Jedes Betriebssystem der SnapCenter Version wird mit den neuesten Sicherheits-Patches aktualisiert, die für maximale Sicherheit verfügbar sind.

NetApp entwickelt Softwarefunktionen und Sicherheits-Patches zu den SnapCenter Plug-ins für die VMware vSphere Appliance und gibt sie anschließend dem Kunden als gebündelte Software-Plattform frei. Da diese Appliances bestimmte Linux Unterbetriebssystem-Abhängigkeiten sowie unsere proprietäre Software umfassen, empfiehlt NetApp, am Unterbetriebssystem keine Änderungen vorzunehmen, da dies ein hohes Potenzial hat, die NetApp Appliance zu beeinträchtigen. Dies könnte sich darauf auswirken, inwieweit NetApp die Appliance unterstützt. NetApp empfiehlt, unsere neueste Code-Version für Appliances zu testen und zu implementieren, da sie veröffentlicht werden, um sicherheitsbezogene Probleme zu patchen.