產品安全性
Enterprise applications

NetApp
May 09, 2024

目錄

產品安全性

VMware vSphere適用的工具ONTAP

採用 ONTAP Tools for VMware vSphere 的軟體工程採用下列安全開發活動：

- *威脅建模。*威脅建模的目的是在軟體開發生命週期初期、發現某項功能、元件或產品的安全性瑕疵。威脅模式是對影響應用程式安全性的所有資訊的結構化呈現。基本上、它是透過安全性觀點來檢視應用程式及其環境。
- *動態應用程式安全性測試（dast）。*這項技術的設計、是為了偵測應用程式在執行狀態下的易受影響狀況。Dast會測試開放Web應用程式的公開HTTP和HTML介面。
- *協力廠商程式碼貨幣。*在開放原始碼軟體（開放原始碼軟體）的軟體開發過程中、您必須解決與產品內建的任何開放原始碼軟體相關的安全性弱點。這是一項持續努力、因為新的開放源碼版本可能隨時都有新發現的弱點報告。
- *弱點掃描。*弱點掃描的目的是在NetApp產品中發現常見且已知的安全性弱點之後、再將弱點發佈給客戶。
- *滲透測試。*滲透測試是評估系統、Web應用程式或網路以找出攻擊者可能利用的安全性弱點的程序。NetApp的滲透測試（筆測試）是由一群獲核准且值得信賴的第三方公司進行。其測試範圍包括利用精密的利用方法或工具、對類似於惡意入侵者或駭客的應用程式或軟體發動攻擊。

產品安全功能

適用於 VMware vSphere 的 ONTAP 工具在每個版本中都包含下列安全功能。

- 登入橫幅。 SSH預設為停用、如果從VM主控台啟用、則僅允許一次性登入。使用者在登入提示中輸入使用者名稱後、會顯示下列登入橫幅：

  *警告：*禁止未經授權存取本系統、並依法律予以起訴。存取本系統即表示您同意、若懷疑有未獲授權的使用情形、您的行動可能受到監控。

  使用者透過 SSH 通道完成登入後、會顯示下列文字：

```
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.
```

- 角色型存取控制（**RBAC**）。 ONTAP 有兩種RBAC控制項與VMware Tools相關聯：
  - 原生vCenter Server權限
  - vCenter外掛程式特定權限。如需詳細資訊、請參閱 "此連結"。
- *加密的通訊通道。*所有外部通訊都是透過使用TLS 1.2版的HTTPS進行。
- *最小的連接埠曝光。*只有必要的連接埠會在防火牆上開啟。

下表說明開放連接埠的詳細資料。

TCP v4/v6連接埠#	方向	功能
8143.	傳入	用於REST API的HTTPS連線
8043.	傳入	HTTPS連線
9060	傳入	HTTPS連線 用於透過 https 連線的 SOAP 此連接埠必須開啟、才能讓用戶端連線至 ONTAP 工具 API 伺服器。
22	傳入	SSH（預設為停用）
9080	傳入	HTTPS連線- VP和SRA -僅從回送進行內部連線
9083.	傳入	HTTPS 連線： VP 與 SRA 用於透過 https 連線的 SOAP
1162	傳入	VP SNMP設陷封包
1527.	僅限內部使用	僅在此電腦與本身之間的外部連線不接受（僅限內部連線）
443..	雙向	用於連線ONTAP 至叢集

- 支援憑證授權單位（**CA**）簽署的憑證。 ONTAP VMware vSphere的各種工具支援CA簽署的憑證。請參閱 "知識庫文章" 以取得更多資訊。
- *稽核記錄。*您可以下載支援套裝組合、而且內容極為詳細。使用者登入和登出活動會記錄在個別的記錄檔中。ONTAPVASA API呼叫會記錄在專屬的VASA稽核記錄（本機CXF.log）中。
- *密碼原則。*遵循下列密碼原則：
  - 密碼不會記錄在任何記錄檔中。
  - 密碼不會以純文字形式傳達。
  - 密碼是在安裝程序本身期間設定的。
  - 密碼歷程記錄是可設定的參數。
  - 密碼最短使用期限設為24小時。
  - 密碼欄位的自動完成功能已停用。
  - 利用SHA256雜湊功能、將所有儲存的認證資訊加密。ONTAP

SnapCenter 外掛程式 VMware vSphere

適用於VMware vSphere軟體工程的NetApp SnapCenter 支援外掛程式使用下列安全開發活動：

- *威脅建模。*威脅建模的目的是在軟體開發生命週期初期、發現某項功能、元件或產品的安全性瑕疵。威脅模式是對影響應用程式安全性的所有資訊的結構化呈現。基本上、它是透過安全性觀點來檢視應用程式及其環境。

- *動態應用程式安全性測試（dast）。*專為偵測應用程式執行狀態中的易受影響狀況而設計的技術。Dast會測試開放Web應用程式的公開HTTP和HTML介面。
- *協力廠商程式碼貨幣。*在開發軟體及使用開放原始碼軟體（開放原始碼軟體）的過程中、必須解決與產品整合的開放原始碼軟體（開放原始碼軟體）相關的安全性弱點。這是一項持續努力、因為開放源碼軟體會元件的版本可能隨時報告新發現的弱點。
- *弱點掃描。*弱點掃描的目的是在NetApp產品中發現常見且已知的安全性弱點之後、再將弱點發佈給客戶。
- *滲透測試。*滲透測試是評估系統、Web應用程式或網路以找出攻擊者可能利用的安全性弱點的程序。NetApp的滲透測試（筆測試）是由一群獲核准且值得信賴的第三方公司進行。其測試範圍包括利用精密的利用方法或工具、對惡意入侵者或駭客等應用程式或軟體發動攻擊。
- * 產品安全性事件回應活動。 * 公司內部和外部都發現安全性弱點、如果未及時解決、可能會對 NetApp 的聲譽造成嚴重風險。為了推動此程序、產品安全性事件回應團隊（PSIRT）會報告並追蹤弱點。

產品安全功能

適用於VMware vSphere的NetApp SnapCenter VMware vCenter外掛程式在每個版本中都包含下列安全功能：

- 受限的**Shell**存取。 SSH預設為停用、且只有在從VM主控台啟用時、才允許一次性登入。
- *登入橫幅中的存取警告。*使用者在登入提示中輸入使用者名稱後、會顯示下列登入橫幅：

  *警告：*禁止未經授權存取本系統、並依法律予以起訴。存取本系統即表示您同意、若懷疑有未獲授權的使用情形、您的行動可能受到監控。

  使用者透過SSH通道完成登入後、會顯示下列輸出：

```
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.
```

- 角色型存取控制（**RBAC**）。 ONTAP 有兩種RBAC控制項與VMware Tools相關聯：
  - 原生vCenter Server權限。
  - VMware vCenter外掛程式特定權限。如需詳細資訊、請參閱 "角色型存取控制（RBAC）"。
- *加密的通訊通道。*所有外部通訊都是使用TLS透過HTTPS進行。
- *最小的連接埠曝光。*只有必要的連接埠會在防火牆上開啟。

下表提供開放連接埠詳細資料。

TCP v4/v6連接埠號碼	功能
8144.	用於REST API的HTTPS連線
8080	用於OVA GUI的HTTPS連線
22	SSH（預設為停用）

TCP v4/v6連接埠號碼	功能
3306.	MySQL（僅限內部連線；預設為停用外部連線）
443..	Ngin像（資料保護服務）

- 支援憑證授權單位（**CA**）簽署的憑證。 SnapCenter VMware vSphere的支援外掛程式支援CA簽署憑證的功能。請參閱 "如何建立及/或將SSL憑證匯入SnapCenter VMware vSphere（選擇控制器）的VMware外掛程式"。
- *密碼原則。*下列密碼原則有效：
  - 密碼不會記錄在任何記錄檔中。
  - 密碼不會以純文字形式傳達。
  - 密碼是在安裝程序本身期間設定的。
  - 所有認證資訊均使用SHA256雜湊來儲存。
- 基本作業系統映像。*本產品隨附適用於OVA的Debian基礎作業系統、存取受限且停用Shell存取。如此可減少攻擊佔用空間。每SnapCenter 個發行版基礎作業系統都會更新最新的安全修補程式、以達到最大的安全覆蓋範圍。

NetApp針對SnapCenter VMware vSphere應用裝置開發有關VMware vSphere外掛程式的軟體功能與安全性修補程式、然後將其作為套裝軟體平台發佈給客戶。由於這些應用裝置包括特定的Linux子作業系統相依性、以及我們的專屬軟體、因此NetApp建議您不要變更子作業系統、因為這會對NetApp應用裝置造成重大影響。這可能會影響NetApp支援應用裝置的能力。NetApp建議測試及部署我們最新的應用裝置程式碼版本、因為這些版本已發行以修補任何與安全性相關的問題。