Seguridad de los productos

Enterprise applications

NetApp
May 09, 2024

Tabla de contenidos

Seguridad de los productos

Herramientas de ONTAP para VMware vSphere

La ingeniería de software con Herramientas de ONTAP para VMware vSphere emplea las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** esta tecnología está diseñada para detectar condiciones vulnerables en aplicaciones en su estado de funcionamiento. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software con software de código abierto (OSS), debe tratar las vulnerabilidades de seguridad que pueden estar asociadas con cualquier OSS incorporado en su producto. Esto es un esfuerzo continuo porque una nueva versión de OSS podría tener una vulnerabilidad recién descubierta reportada en cualquier momento.
- **Análisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- * Pruebas de penetración.* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. Su alcance de prueba incluye el lanzamiento de ataques contra una aplicación o software similar a intrusos hostiles o piratas informáticos que utilizan métodos o herramientas de explotación sofisticados.

Funciones de seguridad de los productos

Las herramientas de ONTAP para VMware vSphere incluyen las siguientes funciones de seguridad en cada versión.

- **Banner de inicio de sesión.** SSH está desactivado de forma predeterminada y sólo permite inicios de sesión de una vez si está activado desde la consola de VM. Se muestra el siguiente banner de inicio de sesión una vez que el usuario introduce un nombre de usuario en la solicitud de inicio de sesión:

  ADVERTENCIA: el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

  Una vez que el usuario complete el inicio de sesión a través del canal SSH, se muestra el siguiente texto:

```
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.
```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server
  - Privilegios específicos del plugin de vCenter. Para obtener más información, consulte "este enlace".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando la versión 1.2 de TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

  En la siguiente tabla se describen los detalles de los puertos abiertos.

Puerto TCP v4/v6 #	Dirección	Función
8143	entrante	Conexiones HTTPS para la API de REST
8043	entrante	Conexiones HTTPS
9060	entrante	Conexiones HTTPS Se utiliza para conexiones SOAP a través de https Este puerto se debe abrir para permitir que un cliente se conecte al servidor API de herramientas de ONTAP.
22	entrante	SSH (deshabilitado de forma predeterminada)
9080	entrante	Conexiones HTTPS - VP y SRA - conexiones internas sólo del bucle invertido
9083	entrante	Conexiones HTTPS: VP y SRA Se utiliza para conexiones SOAP a través de https
1162	entrante	VP paquetes de captura SNMP
1527	exclusivamente para uso interno	Puerto de base de datos Derby, sólo entre este equipo y él mismo, no se aceptan conexiones externas — sólo conexiones internas

Puerto TCP v4/v6 #	Dirección	Función
443	bidireccional	Se utiliza para las conexiones a clústeres de ONTAP

- **Compatibilidad con certificados firmados por la entidad de certificación (CA).** las herramientas de ONTAP para VMware vSphere admiten certificados firmados por CA. Vea esto "artículo de base de conocimientos" si quiere más información.
- **Registro de auditoría.** los paquetes de soporte se pueden descargar y son extremadamente detallados. Las herramientas de ONTAP registran toda la actividad de inicio de sesión y cierre de sesión de los usuarios en un archivo de registro independiente. Las llamadas de API VASA se registran en un registro de auditoría de VASA dedicado (cxf.log local).
- **Políticas de contraseña.** se siguen las siguientes directivas de contraseñas:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - El historial de contraseñas es un parámetro configurable.
  - La antigüedad mínima de la contraseña se establece en 24 horas.
  - El proceso de finalización automática de los campos de contraseña está desactivado.
  - Las herramientas de ONTAP cifran toda la información de credenciales almacenada mediante el hash SHA256.

Complemento de SnapCenter, VMware vSphere

La ingeniería de software del complemento SnapCenter de NetApp para VMware vSphere utiliza las siguientes actividades de desarrollo seguro:

- **Modelado de amenazas.** el propósito del modelado de amenazas es descubrir defectos de seguridad en una característica, componente o producto al principio del ciclo de vida del desarrollo del software. Un modelo de amenaza es una representación estructurada de toda la información que afecta la seguridad de una aplicación. En esencia, es una visión de la aplicación y su entorno a través del objetivo de la seguridad.
- **Pruebas de seguridad de aplicaciones dinámicas (DAST).** Tecnologías diseñadas para detectar condiciones vulnerables en aplicaciones en estado en ejecución. DAST prueba las interfaces HTTP y HTML expuestas de las aplicaciones web.
- **Moneda de código de terceros.** como parte del desarrollo de software y el uso de software de código abierto (OSS), es importante abordar las vulnerabilidades de seguridad que pueden estar asociadas con OSS que se han incorporado a su producto. Se trata de un esfuerzo continuo, ya que la versión del componente OSS puede tener una vulnerabilidad recién descubierta reportada en cualquier momento.
- **Análisis de vulnerabilidades.** el propósito del análisis de vulnerabilidades es detectar vulnerabilidades de seguridad comunes y conocidas en los productos de NetApp antes de que se lancen a los clientes.
- * Pruebas de penetración.* la prueba de penetración es el proceso de evaluar un sistema, una aplicación web o una red para encontrar vulnerabilidades de seguridad que podrían ser explotadas por un atacante. Las pruebas de penetración (pruebas de Pen) en NetApp las realiza un grupo de empresas de terceros aprobadas y fiables. El alcance de su prueba incluye el lanzamiento de ataques contra una aplicación o software como intrusos hostiles o hackers que utilizan métodos o herramientas de explotación sofisticados.

- * Actividad de respuesta a incidentes de seguridad de los productos.* Las vulnerabilidades de seguridad se detectan tanto interna como externamente en la empresa y pueden representar un riesgo grave para la reputación de NetApp si no se tratan de manera puntual. Para facilitar este proceso, un equipo de respuesta a incidentes de seguridad de productos (PSIRT) informa y realiza un seguimiento de las vulnerabilidades.

Funciones de seguridad de los productos

El plugin de SnapCenter de NetApp para VMware vSphere incluye las siguientes funciones de seguridad en cada versión:

- **Acceso restringido al shell.** SSH está desactivado de forma predeterminada, y sólo se permiten inicios de sesión una vez si están habilitados desde la consola de VM.
- **Advertencia de acceso en el banner de inicio de sesión.** se muestra el siguiente banner de inicio de sesión después de que el usuario introduzca un nombre de usuario en el indicador de inicio de sesión:

  ADVERTENCIA: el acceso no autorizado a este sistema está prohibido y será procesado por ley. Al acceder a este sistema, acepta que sus acciones pueden supervisarse si se sospecha un uso no autorizado.

  Una vez que el usuario completa el inicio de sesión a través del canal SSH, se muestra la siguiente salida:

```
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.
```

- **Control de acceso basado en roles (RBAC).** dos tipos de controles RBAC están asociados con las herramientas ONTAP:
  - Privilegios nativos de vCenter Server.
  - Privilegios específicos del complemento de VMware vCenter. Para obtener más información, consulte "Control de acceso basado en roles (RBAC)".
- **Canales de comunicaciones cifrados.** toda comunicación externa ocurre a través de HTTPS utilizando TLS.
- **Exposición mínima del puerto.** sólo los puertos necesarios están abiertos en el firewall.

En la siguiente tabla se proporcionan los detalles de los puertos abiertos.

Número de puerto TCP v4/v6	Función
8144	Conexiones HTTPS para la API de REST
8080	Conexiones HTTPS para interfaz gráfica de usuario de OVA
22	SSH (deshabilitado de forma predeterminada)

Número de puerto TCP v4/v6	Función
3306	MySQL (sólo conexiones internas; las conexiones externas están deshabilitadas de forma predeterminada)
443	Nginx (servicios de protección de datos)

- **Compatibilidad con certificados firmados por entidad de certificación (CA).** el plugin de SnapCenter para VMware vSphere es compatible con la función de certificados firmados por CA. Consulte "Cómo crear o importar un certificado SSL al plugin de SnapCenter para VMware vSphere (SCV)".
- **Políticas de contraseña.** las siguientes directivas de contraseñas están en vigor:
  - Las contraseñas no han iniciado sesión en ningún archivo de registro.
  - Las contraseñas no se comunican en texto sin formato.
  - Las contraseñas se configuran durante el propio proceso de instalación.
  - Toda la información de credenciales se almacena mediante el hash SHA256.
- **Imagen del sistema operativo base.** el producto se entrega con el SO base Debian para OVA con acceso restringido y acceso al shell desactivado. Esto reduce el espacio necesario para los ataques. Todos los sistemas operativos base de la versión SnapCenter se actualizan con los parches de seguridad más recientes disponibles para obtener la máxima cobertura de seguridad.

NetApp desarrolla funciones de software y parches de seguridad con respecto al dispositivo del plugin de SnapCenter para VMware vSphere y, a continuación, se los libera a los clientes como una plataforma de software integrada. Dado que estos dispositivos incluyen dependencias específicas de sistemas suboperativos de Linux y nuestro software exclusivo, NetApp recomienda no realizar cambios en el sistema operativo de subsistema, ya que esto tiene un gran potencial para afectar al dispositivo de NetApp. Esto podría afectar a la capacidad de NetApp para dar soporte al dispositivo. NetApp recomienda probar e implementar nuestra última versión de código para los dispositivos, ya que se los publica para resolver cualquier problema relacionado con la seguridad.

Información de copyright

Información de la marca comercial