Sicurezza dei prodotti

Enterprise applications

NetApp
May 09, 2024

Sommario

Sicurezza dei prodotti

Strumenti ONTAP per VMware vSphere

La progettazione software con strumenti ONTAP per VMware vSphere si avvale delle seguenti attività di sviluppo sicure:

- **Modellazione delle minacce.** lo scopo della modellazione delle minacce è quello di individuare i difetti di sicurezza in una funzionalità, un componente o un prodotto nelle prime fasi del ciclo di vita dello sviluppo software. Un modello di minaccia è una rappresentazione strutturata di tutte le informazioni che influiscono sulla sicurezza di un'applicazione. In sostanza, si tratta di una vista dell'applicazione e del suo ambiente attraverso l'obiettivo della sicurezza.
- **Dynamic Application Security Testing (DAST).** questa tecnologia è progettata per rilevare le condizioni vulnerabili delle applicazioni in esecuzione. DAST testa le interfacce HTTP e HTML esposte delle applicazioni web-enable.
- **Valuta del codice di terze parti.** nell'ambito dello sviluppo di software con software open-source (OSS), è necessario risolvere le vulnerabilità di sicurezza che potrebbero essere associate a qualsiasi OSS incorporato nel prodotto. Si tratta di un'operazione continua, in quanto una nuova versione di OSS potrebbe presentare una vulnerabilità scoperta di recente in qualsiasi momento.
- **Scansione delle vulnerabilità.** lo scopo della scansione delle vulnerabilità è quello di rilevare vulnerabilità di sicurezza comuni e note nei prodotti NetApp prima che vengano rilasciate ai clienti.
- Test di penetrazione.* il test di penetrazione è il processo di valutazione di un sistema, di un'applicazione Web o di una rete per individuare le vulnerabilità di sicurezza che potrebbero essere sfruttate da un utente malintenzionato. I test di penetrazione (test delle penne) di NetApp vengono condotti da un gruppo di aziende terze approvate e fidate. Il loro scopo di test include il lancio di attacchi contro un'applicazione o un software simile a intrusi o hacker ostili che utilizzano sofisticati metodi o strumenti di sfruttamento.

Funzionalità di sicurezza del prodotto

I tool ONTAP per VMware vSphere includono le seguenti funzionalità di sicurezza in ciascuna release.

- **Login banner.** SSH è disattivato per impostazione predefinita e consente l'accesso una sola volta, se abilitato dalla console della macchina virtuale. Il seguente banner di accesso viene visualizzato dopo che l'utente ha inserito un nome utente nel prompt di accesso:

  ATTENZIONE: l'accesso non autorizzato a questo sistema è vietato e sarà perseguito dalla legge. Accedendo a questo sistema, l'utente accetta che le proprie azioni possano essere monitorate in caso di sospetto di utilizzo non autorizzato.

  Dopo che l'utente ha completato l'accesso tramite il canale SSH, viene visualizzato il seguente testo:

```
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.
```

- **RBAC (role-based access control).** due tipi di controlli RBAC sono associati ai tool ONTAP:
  - Privilegi vCenter Server nativi
  - Privilegi specifici del plug-in vCenter. Per ulteriori informazioni, vedere "questo link".
- **Canali di comunicazione crittografati.** tutte le comunicazioni esterne avvengono su HTTPS utilizzando la versione 1.2 di TLS.
- **Esposizione minima delle porte.** solo le porte necessarie sono aperte sul firewall.

  La seguente tabella descrive i dettagli della porta aperta.

Porta TCP v4/v6 n.	Direzione	Funzione
8143	in entrata	Connessioni HTTPS per API REST
8043	in entrata	Connessioni HTTPS
9060	in entrata	Connessioni HTTPS Utilizzato per connessioni SOAP su https Questa porta deve essere aperta per consentire a un client di connettersi al server API degli strumenti ONTAP.
22	in entrata	SSH (Disattivato per impostazione predefinita)
9080	in entrata	Connessioni HTTPS - VP e SRA - connessioni interne solo da loopback
9083	in entrata	Connessioni HTTPS - VP e SRA Utilizzato per connessioni SOAP su https
1162	in entrata	Pacchetti di trap SNMP VP
1527	solo interno	Porta del database Derby, solo tra questo computer e se stesso, connessioni esterne non accettate — solo connessioni interne
443	bidirezionale	Utilizzato per le connessioni ai cluster ONTAP

- **Supporto dei certificati firmati dall'autorità di certificazione (CA).** i tool ONTAP per VMware vSphere supportano i certificati firmati CA. Vedi questo "articolo della knowledge base" per ulteriori informazioni.
- **Registrazione audit.** i pacchetti di supporto possono essere scaricati e sono estremamente dettagliati. ONTAP Tools registra tutte le attività di login e logout degli utenti in un file di log separato. Le chiamate API VASA vengono registrate in un registro di controllo VASA dedicato (cxf.log locale).
- **Criteri per le password.** vengono seguite le seguenti policy per le password:
  - Le password non vengono registrate in alcun file di log.
  - Le password non vengono comunicate in testo normale.

- Le password vengono configurate durante il processo di installazione.
- La cronologia delle password è un parametro configurabile.
- La durata minima della password è impostata su 24 ore.
- Il completamento automatico dei campi della password è disattivato.
- Gli strumenti ONTAP crittografano tutte le informazioni sulle credenziali memorizzate utilizzando l'hashing SHA256.

Plug-in di SnapCenter per VMware vSphere

Il plug-in NetApp SnapCenter per il software engineering VMware vSphere utilizza le seguenti attività di sviluppo sicuro:

- **Modellazione delle minacce.** lo scopo della modellazione delle minacce è quello di individuare i difetti di sicurezza in una funzionalità, un componente o un prodotto nelle prime fasi del ciclo di vita dello sviluppo software. Un modello di minaccia è una rappresentazione strutturata di tutte le informazioni che influiscono sulla sicurezza di un'applicazione. In sostanza, si tratta di una vista dell'applicazione e del suo ambiente attraverso l'obiettivo della sicurezza.
- **Dynamic Application Security testing (DAST).** tecnologie progettate per rilevare condizioni vulnerabili sulle applicazioni in esecuzione. DAST testa le interfacce HTTP e HTML esposte delle applicazioni web-enable.
- **Valuta del codice di terze parti.** come parte dello sviluppo di software e dell'utilizzo di software open-source (OSS), è importante risolvere le vulnerabilità di sicurezza che potrebbero essere associate a OSS che è stato incorporato nel prodotto. Si tratta di un impegno continuo, in quanto la versione del componente OSS potrebbe presentare una vulnerabilità scoperta di recente in qualsiasi momento.
- **Scansione delle vulnerabilità.** lo scopo della scansione delle vulnerabilità è quello di rilevare vulnerabilità di sicurezza comuni e note nei prodotti NetApp prima che vengano rilasciate ai clienti.
- Test di penetrazione.* il test di penetrazione è il processo di valutazione di un sistema, di un'applicazione Web o di una rete per individuare le vulnerabilità della sicurezza che potrebbero essere sfruttate da un utente malintenzionato. I test di penetrazione (test delle penne) di NetApp vengono condotti da un gruppo di aziende terze approvate e fidate. Il loro scopo di test include il lancio di attacchi contro un'applicazione o un software come intrusi o hacker ostili che utilizzano sofisticati metodi o strumenti di sfruttamento.
- **Attività di risposta agli incidenti di sicurezza dei prodotti.** le vulnerabilità di sicurezza sono scoperte sia internamente che esternamente all'azienda e possono rappresentare un serio rischio per la reputazione di NetApp se non vengono affrontate in modo tempestivo. Per facilitare questo processo, un Product Security Incident Response Team (PSIRT) segnala e tiene traccia delle vulnerabilità.

Funzionalità di sicurezza del prodotto

Il plug-in NetApp SnapCenter per VMware vSphere include le seguenti funzionalità di sicurezza in ciascuna release:

- **Accesso limitato alla shell.** SSH è disattivato per impostazione predefinita e gli accessi una tantum sono consentiti solo se sono abilitati dalla console della macchina virtuale.
- **Avviso di accesso nel banner di accesso.** il seguente banner di accesso viene visualizzato dopo che l'utente ha inserito un nome utente nel prompt di accesso:

  ATTENZIONE: l'accesso non autorizzato a questo sistema è vietato e sarà perseguito dalla legge. Accedendo a questo sistema, l'utente accetta che le proprie azioni possano essere monitorate in caso di sospetto di utilizzo non autorizzato.

Una volta completato l'accesso tramite il canale SSH, viene visualizzato il seguente output:

```
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.
```

- **RBAC (role-based access control).** due tipi di controlli RBAC sono associati ai tool ONTAP:
  - Privilegi vCenter Server nativi.
  - Privilegi specifici del plug-in VMware vCenter. Per ulteriori informazioni, vedere "RBAC (Role-Based Access Control)".
- **Canali di comunicazione crittografati.** tutte le comunicazioni esterne avvengono su HTTPS utilizzando TLS.
- **Esposizione minima delle porte.** solo le porte necessarie sono aperte sul firewall.

La seguente tabella fornisce i dettagli della porta aperta.

Numero della porta TCP v4/v6	Funzione
8144	Connessioni HTTPS per API REST
8080	Connessioni HTTPS per GUI OVA
22	SSH (disattivato per impostazione predefinita)
3306	MySQL (solo connessioni interne; connessioni esterne disattivate per impostazione predefinita)
443	Nginx (servizi di protezione dei dati)

- **Supporto dei certificati firmati dall'autorità di certificazione (CA).** il plug-in SnapCenter per VMware vSphere supporta la funzione dei certificati firmati dalla CA. Vedere "Come creare e/o importare un certificato SSL nel plug-in SnapCenter per VMware vSphere (SCV)".
- **Password policy.** sono in vigore i seguenti criteri relativi alle password:
  - Le password non vengono registrate in alcun file di log.
  - Le password non vengono comunicate in testo normale.
  - Le password vengono configurate durante il processo di installazione.
  - Tutte le informazioni sulle credenziali vengono memorizzate utilizzando l'hashing SHA256.
- **Immagine del sistema operativo di base.** il prodotto viene fornito con il sistema operativo di base Debian per OVA con accesso limitato e accesso alla shell disattivato. In questo modo si riduce l'impatto degli attacchi. Ogni sistema operativo SnapCenter release base viene aggiornato con le ultime patch di sicurezza disponibili per la massima copertura di sicurezza.

NetApp sviluppa funzionalità software e patch di sicurezza per quanto riguarda il plug-in SnapCenter per l'appliance VMware vSphere e le rilascia ai clienti come piattaforma software integrata. Poiché queste appliance includono dipendenze specifiche del sistema operativo secondario Linux e il nostro software

proprietario, NetApp consiglia di non apportare modifiche al sistema operativo secondario, in quanto questo potrebbe influire sull'appliance NetApp. Ciò potrebbe influire sulla capacità di NetApp di supportare l'appliance. NetApp consiglia di testare e implementare la versione più recente del codice per le appliance, perché vengono rilasciate per correggere eventuali problemi relativi alla sicurezza.