

Accesso VPN AnyConnect Secure Client negato a causa di problemi di conformità della postura di sicurezza degli endpoint

Sommario

Problema

Più utenti non possono connettersi ad AnyConnect VPN e Zero Trust Access (ZTA) e ricevere il messaggio di errore "Accesso negato. L'ambiente non soddisfa i criteri di accesso definiti dall'amministratore."

Il problema è correlato alla conformità della postura dell'endpoint, in cui il requisito dell'agente di sicurezza dell'endpoint viene segnalato come non corrispondente. Gli utenti riscontrano un rifiuto di accesso VPN e ZTA quando tentano di connettersi tramite Cisco Secure Client.

La valutazione della postura indica che la postura di Trellix Endpoint Security ha esito negativo sugli endpoint interessati, impedendo la corretta autenticazione al servizio VPN.

Ambiente

- Cisco Secure Client (AnyConnect e Zero Trust Access)
- Trellix Endpoint Security Agent versione 5.8.4.505
- Profilo postura VPN: KFIN_SECURE_VPN con imposizione dell'agente di sicurezza dell'endpoint
- Requisito postura: Agente di sicurezza degli endpoint in esecuzione con aggiornamenti negli ultimi 14 giorni
- Endpoint Windows con servizio agente Trellix in esecuzione
- Rilevati processi di Umbrella Agent sugli endpoint

Risoluzione

Il problema è stato risolto risolvendo i problemi di conformità della postura dell'agente Trellix Endpoint Security. Sono stati implementati i passaggi per la risoluzione dei problemi descritti nelle sezioni seguenti.

Passaggio 1: Convalida configurazione profilo postura

Rivedere il profilo di postura VPN per confermare i requisiti dell'agente di sicurezza dell'endpoint. Il profilo KFIN_SECURE_VPN impone che un agente di sicurezza dell'endpoint sia in esecuzione e aggiornato negli ultimi 14 giorni.

Passaggio 2: Verifica stato sicurezza endpoint Trellix

Verificare lo stato corrente dell'agente Trellix Endpoint Security sugli endpoint interessati:

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

Passaggio 3: Reinstalla Trellix Endpoint Security

Eseguire una reinstallazione completa di Trellix Endpoint Security sugli endpoint interessati:

1. Disinstallare completamente l'agente Trellix Endpoint Security esistente.
2. Riavviare il sistema.
3. Installare l'ultima versione approvata dell'agente Trellix in base agli standard dell'organizzazione.

4. Verificare che l'agente sia in esecuzione dopo l'installazione.

5. Confermare il completamento degli aggiornamenti di firma/contenuto.

Passaggio 4: Abilita registrazione TRACCIA per Cisco Secure Client (ZTA)

Abilitare la registrazione dettagliata per acquisire i dettagli di valutazione della postura.

Creare il file logconfig.json con il seguente contenuto:

```
{ "global": "DBG_TRACE" }
```

Posizionare il file nella directory appropriata:

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS: /opt/cisco/secureclient/zta

Riavviare il servizio Cisco Secure Client/ZTA dopo aver creato il file.

Passaggio 5: Raccogli pacchetto DART aggiornato

Dopo aver implementato le modifiche, raccogliete un nuovo bundle DART per convalidare la risoluzione e confermare il corretto rilevamento della conformità della postura.

Causa

La causa principale è stata identificata come un problema di conformità alla postura dell'agente di sicurezza degli endpoint Trellix. Il profilo di postura VPN ha richiesto l'esecuzione di un agente di sicurezza endpoint con aggiornamenti negli ultimi 14 giorni, ma l'agente di sicurezza endpoint Trellix non soddisfa questi criteri di conformità. Il modulo di valutazione della postura non è stato in grado di rilevare o convalidare correttamente lo stato dell'agente di sicurezza dell'endpoint. Ciò ha

causato il rifiuto dell'accesso per le connessioni VPN e ZTA. Il problema era specificamente correlato alla configurazione dell'agente Trellix e richiedeva l'intervento del team di supporto Trellix per risolvere i problemi di conformità dell'agente sottostante.

Contenuto correlato

- [Raccolta dei log ZTNA dettagliati per la risoluzione dei problemi](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).