Auflösen doppelter ZTNA-Geräte-IDs in Bereitstellungen mit sicherem Zugriff mithilfe von SysPrep Golden Images

Inhalt

Problem

Mehrere physische Windows-Computer, die aus einem goldenen SysPrep-Abbild bereitgestellt werden, generieren identische ZTNA-Geräte-IDs, insbesondere dieselbe ztnaDeviceId für mehrere Endpunkte. Diese Duplizierung verursacht mehrere kritische Probleme:

- Wiederholte erneute Anmeldung von Geräten mit derselben ZTNA-Geräte-ID
- Überschreibungen des öffentlichen Schlüssels bei jedem erneuten Registrierungsprozess
- Statusprüfungsfehler auf allen Computern mit Ausnahme des zuletzt registrierten Geräts
- Zugriffsfehler durch sicheren Zugriff für betroffene Endgeräte

Das beobachtete Verhalten tritt auf, wenn mehrere Maschinen in der Flotte die gleiche ZTNA-Geräte-ID teilen, wodurch jede Anmeldung den öffentlichen Schlüssel der vorherigen Maschine überschreibt. Mit Ausnahme des zuletzt angemeldeten Geräts versenden alle Systeme keine Statusüberprüfungen, was zu einer Zugriffsverweigerung über die Secure Access-Infrastruktur führt.

Mehrere Paare von Hostnamen und Benutzer-IDs wurden als mit derselben ZTNA-Geräte-ID verknüpft identifiziert, was den Umfang des Duplizierungsproblems in der gesamten Bereitstellung verdeutlicht.

Umwelt

- Cisco Secure Access (ZTNA-Implementierung)

- Physische Windows-Systeme (keine virtuellen Systeme)
- SysPrep Gold Image-Bereitstellungsmethode
- Windows ADK-Tools (Assessment and Deployment Kit) für die Image-Bereitstellung
- ESD-Dateiformat (Electronic Software Delivery) für die Bilderfassung
- Standardisierter BS-Härtungsprozess einschließlich obligatorischer Softwareinstallation
- Standardkonfiguration für lokale Administratoren und Gastkonten

Auflösung

Der Auflösungsprozess umfasste eine umfassende Protokollanalyse und die Identifizierung der Ursache durch detaillierte Untersuchungen.

Ursachenermittlung und -beseitigung

Die Untersuchung ergab, dass der SysPrep-Prozess bei der Bereitstellung des Gold Images keine eindeutigen Gerätekennungen erzeugte.

Die Analyse umfasste Folgendes:

Prüfung von Windows-Registrierungsschlüsseln, insbesondere:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
```

Erfassen der Benutzer-Sicherheits-IDs mithilfe von:

```
whoami /user
```

Die Lösung erforderte die Änderung des SysPrep-Prozesses, um sicherzustellen, dass gerätespezifische Identifikatoren während der Bereitstellung ordnungsgemäß regeneriert werden, sodass die Duplizierung von ZTNA-Geräte-IDs über mehrere physische Systeme hinweg

vermieden wird.

- Wenn Sie UDID durch Ausführen des Befehls dartcli.exe -nu erneuern, ändert sich der Wert von Nounce unter dem Registrierungspfad "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails".
- Durch Löschen der JSON-Datei von C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments & Neustart des ZTA-Dienstes wird die Anmeldung des Benutzers aufgehoben. Sie müssen den Benutzer manuell registrieren. Dies erzeugt eine neue JSON-Datei ohne weitere Auswirkungen.
- Die Verlängerung von UDID auf allen Endpunkten darf keine Auswirkungen haben, solange der Wert auf keinem Server überprüft/ausgewertet wird.

1. Starten Sie die Eingabeaufforderung als Administrator, und wechseln Sie zum Verzeichnis "%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART".

2. Führen Sie dartcli.exe -u aus, um den Wert der aktuellen UDID zu überprüfen.

3. Führen Sie den Befehl dartcli.exe -nu aus. Dieser Befehl erneuert die UDID.

4. Überprüfen Sie den neuen Wert, indem Sie den Befehl in Schritt 2 wiederholen.

5. Löschen Sie die JSON-Datei aus dem Verzeichnis C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments

6. Starten Sie die VPN- und ZTA-Dienste neu. Zu diesem Zeitpunkt muss sich ZTA im nicht eingeschriebenen Zustand befinden.

7. Lassen Sie den Benutzer manuell registrieren ZTA

9. Überprüfen Sie den Wert von new ztnaDeviceId in der JSON-Datei.

Überwachung und Validierung

Nach der Implementierung der Korrekturmaßnahmen, um eine eindeutige Generierung der ZTNA-Geräte-ID sicherzustellen:

- Anmeldeprozess über mehrere Systeme hinweg überwacht
- Überprüft, ob von jedem System eindeutige ZTNA-Geräte-IDs generiert wurden.
- Bestätigte Funktionalität der Statusüberprüfung für alle registrierten Geräte
- Validiert, dass die Überschreibungen des öffentlichen Schlüssels während der Registrierung nicht mehr auftraten

Ursache

Die Ursache wurde als "SysPrep Golden Image Deployment" identifiziert, bei dem keine eindeutigen Gerätekennungen für die ZTNA-Registrierung generiert wurden. Wenn mehrere physische Windows-Computer aus demselben goldenen SysPrep-Image bereitgestellt werden, bleiben bestimmte gerätespezifische Bezeichner, die zum Generieren der ZTNA-Geräte-ID verwendet werden, auf allen bereitgestellten Computern identisch.

Der SysPrep-Prozess ist zwar für die Standardisierung der Betriebssystemkonfiguration und Softwarebereitstellung wirksam, wurde jedoch nicht für die Neugenerierung der spezifischen Kennungen konfiguriert, die der Cisco Secure Client zum Erstellen eindeutiger ZTNA-Geräte-IDs verwendet. Dies führte dazu, dass alle Systeme, die von demselben Golden Image bereitgestellt wurden, identische ZTNA-Gerätekennungsparameter erben, was zu Anmeldungskonflikten und Authentifizierungsfehlern in der Secure Access-Infrastruktur führte.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.