

Sicherheitsstatus von Zugriffsgeräten - zeitweilig "veraltet" Fehler

Inhalt

Problem

Der Gerätestatus in Cisco Secure Access zeigt für registrierte Geräte gelegentlich den Status "veraltet" an und verhindert so eine Überprüfung auf den Status "Zero Trust".

Benutzer werden in bestimmten Zeitfenstern mit folgenden Fehlermeldungen konfrontiert:

- "Ihr Gerätestatus ist veraltet"
- "Eine Sicherheitsprüfung für Ihr Gerät konnte nicht automatisch ausgeführt werden."

Das Problem tritt auf, obwohl Duo Desktop angibt, dass alle Sicherheitsanforderungen einschließlich Windows-Updates, Konfiguration des Systemkennworts, BitLocker-Verschlüsselung und Firewall-Aktivierung vollständig erfüllt sind. Während der problematischen Zeiträume schlagen Versuche zum Aufheben und erneuten Registrieren der betroffenen Geräte mit internen Fehlern fehl. Die einzige temporäre Problemumgehung, die den normalen Betrieb wiederherstellt, ist ein vollständiger Systemneustart, der den Benutzerzugriff und die Produktivität unterbricht.

Weitere Symptome sind AnyConnect VPN, das während des gesamten Problemzeitraums die Verbindung aufrechterhält, während die Anmeldung bei Zero Trust Access und die Statusüberprüfung in vorhersehbaren Zeitfenstern periodisch fehlschlagen.

Umwelt

- Cisco Secure Access mit aktivierter Gerätestatusfunktion
- Duo Desktop-Client zur Überprüfung der Geräte-Compliance
- Windows-Endpunkte mit BitLocker-Verschlüsselung, Systemkennwörter und aktivierter

Windows-Firewall

- Bereitstellung ohne Trust Access mit Validierung des Status
- Konfigurierte Statusprofile in Cisco Secure Access stimmen mit dem Konformitätsstatus von Geräten überein

Auflösung

Das Problem wurde durch ein Upgrade des Cisco Secure Access-Clients auf die neueste Version 5.1.15.287 behoben. Diese Version behebt den zugrunde liegenden Fehler, der zu vorübergehenden Fehlern bei der Überprüfung des Gerätestatus führte.

Client-Upgrade-Prozess

Schritt 1: Identifizieren Sie die aktuelle Client-Version auf betroffenen Endgeräten.

Überprüfen Sie die vorhandene Version des Cisco Secure Access-Clients über die Anwendungsschnittstelle oder die Systeminstallationsaufzeichnungen.

Phase 2: Laden Sie die Client-Version 5.1.15.287 herunter, und stellen Sie sie bereit.

Holen Sie die aktualisierte Client-Software vom entsprechenden Cisco Vertriebskanal ein, und stellen Sie sie auf allen betroffenen Endgeräten bereit, bei denen Probleme mit der Gerätestatusüberprüfung auftreten.

Schritt 3: Überprüfen der Auflösung

Überwachen Sie nach Abschluss des Client-Upgrades den Gerätestatus in zuvor problematischen Zeitfenstern, um den stabilen Betrieb zu bestätigen, ohne das System neu zu starten.



Anmerkung: Es wird empfohlen, die neueste Version von Secure Client zu installieren.

Validierungsschritte

Überprüfen Sie nach dem Client-Upgrade Folgendes:

- Die Überprüfung des Gerätestatus wird in zuvor problematischen Zeiträumen erfolgreich abgeschlossen.
- Die Registrierung für den nicht vertrauenswürdigen Zugriff funktioniert ohne interne Fehler.
- Abmeldung und erneute Anmeldung erfolgreich abgeschlossen, wenn erforderlich.
- Es sind keine Systemneustarts erforderlich, um die Einhaltung des Gerätestatus zu gewährleisten.
- Der Status von Duo Desktop und Cisco Secure Access bleibt synchronisiert.

Ursache

Die zeitweiligen Fehler bei der Überprüfung des Gerätestatus wurden durch den Cisco Bug CSCws68569 verursacht. Dieser Fehler beeinträchtigte die Kommunikation zwischen dem Cisco Secure Access-Client und den Statusüberprüfungsdiensten und führte zu vorübergehenden Synchronisierungsproblemen, die eine genaue Meldung des Gerätekonformitätsstatus während bestimmter Betriebsfenster verhinderten.

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.