Sichere Endgeräte - Connector-Updates werden aufgrund der geringeren Angriffsfläche von Microsoft blockiert

Inhalt

Einleitung

In diesem Dokument werden Probleme beschrieben, die durch Oberflächenreduktionsblöcke von Microsoft Intune Attack verursacht werden, indem kopierte oder imitierte System-Tools auf von Microsoft Intune verwalteten Systemen verwendet werden, was wiederum dazu führt, dass Updates für sichere Endpunkte fehlschlagen.

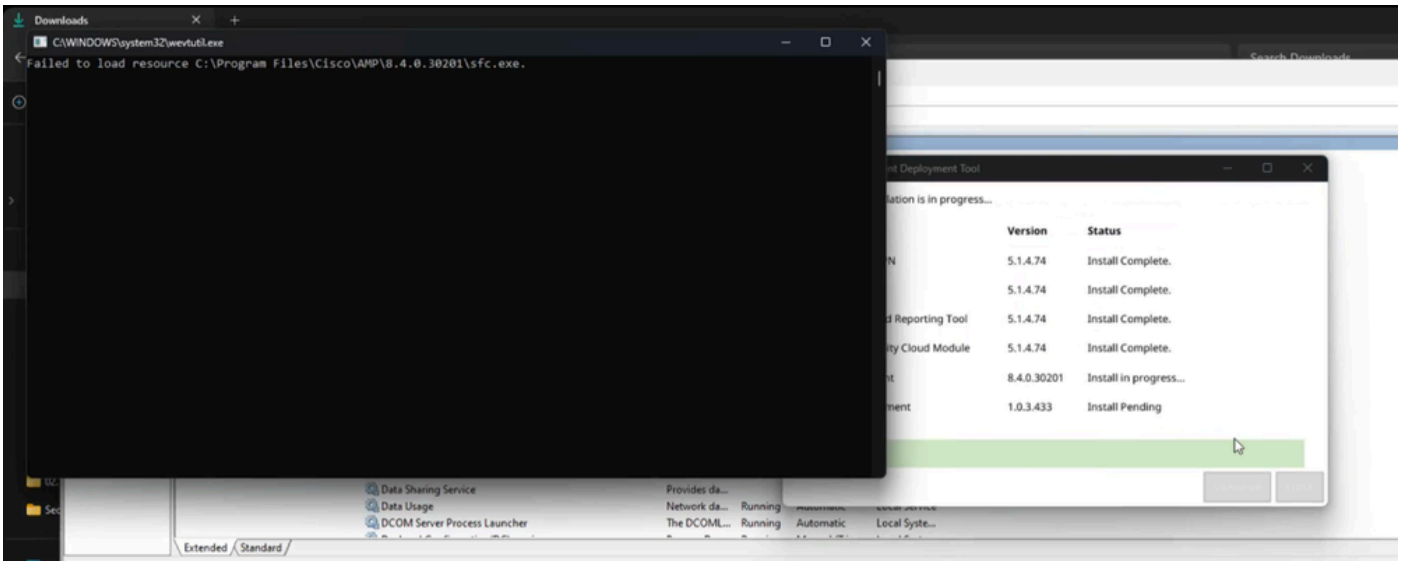
Weitere Informationen finden Sie in der Funktionsdokumentation unter: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

Problem

Es können Probleme mit Secure Endpoint-Upgrades oder -Installationen auftreten, die durch diese Fehler und Indikatoren dargestellt werden.

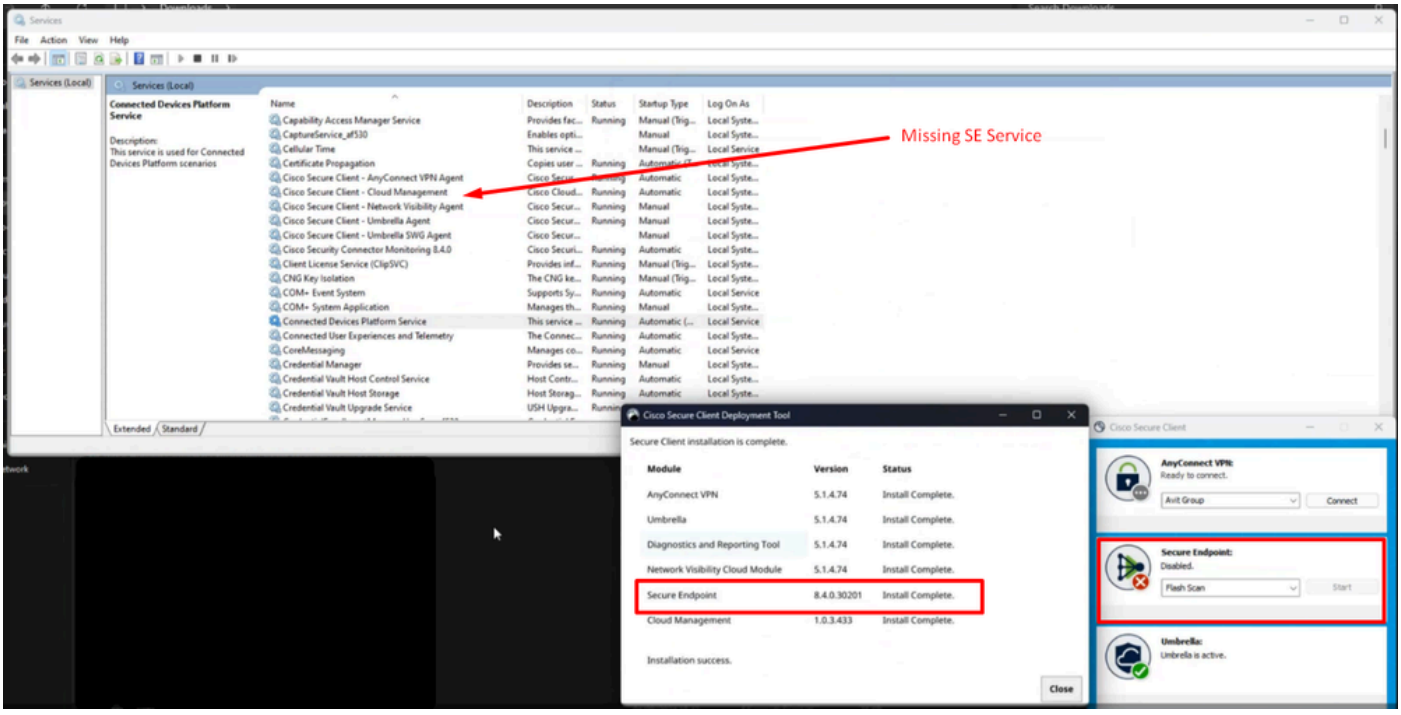
Es gibt verschiedene Indikatoren, anhand derer festgestellt werden kann, dass diese Funktion Sicherheitsaktualisierungen von Endgeräten beeinträchtigt.

Indikator #1: Während der Bereitstellung wird dieses Popup-Fenster am Ende der Installation angezeigt. Bitte beachten Sie, dass das Pop-up ziemlich schnell ist und es keine andere Erinnerung an irgendeinen Fehler gibt, sobald die Installation abgeschlossen ist.

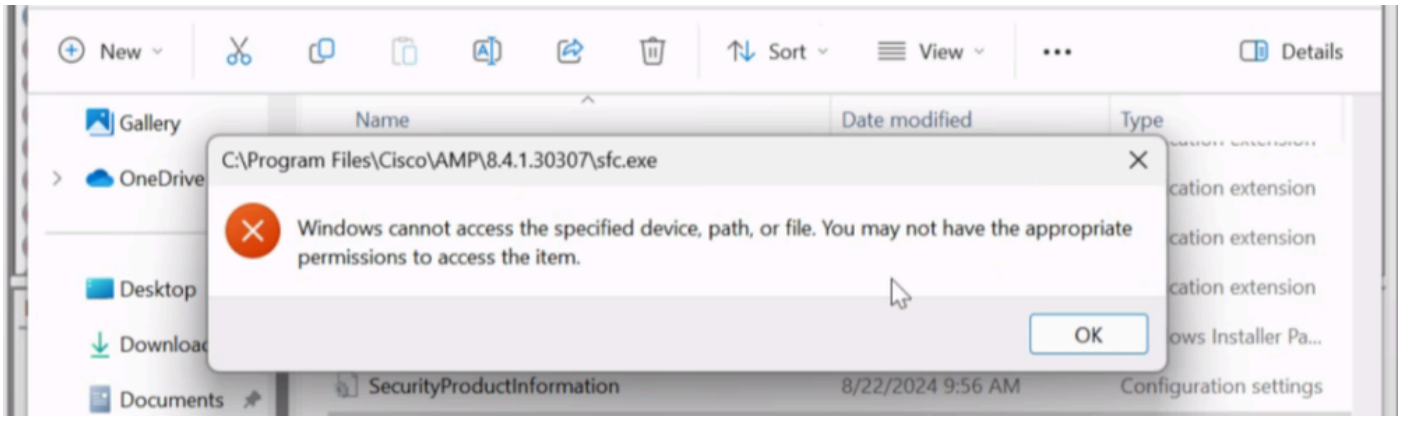


Indikator #2: Beachten Sie nach der Installation, dass Secure Endpoint in der Benutzeroberfläche deaktiviert ist.

Außerdem fehlt Secure Endpoint Service (sfc.exe) im Task-Manager vollständig — > Dienste



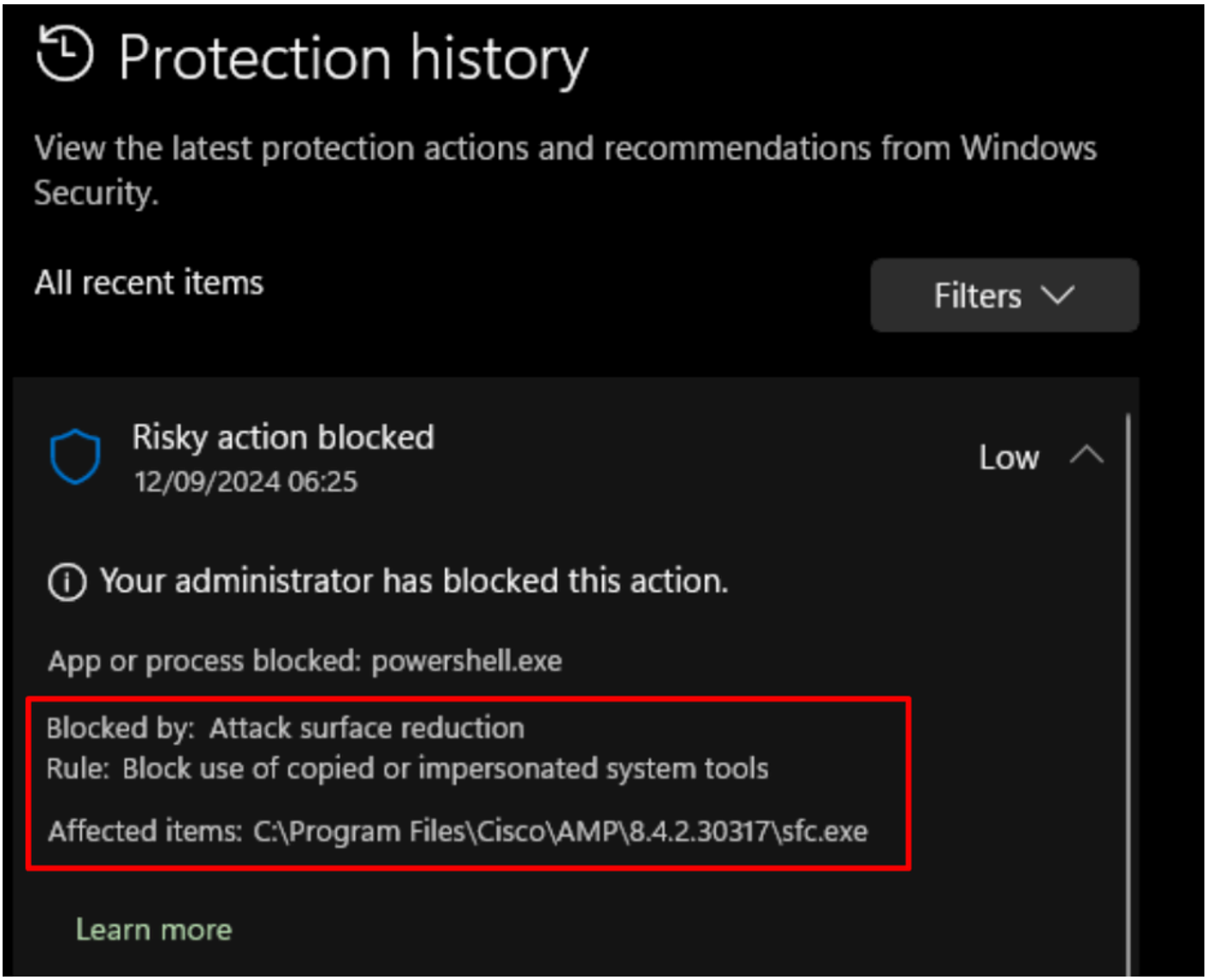
Indikator #3: Wenn wir zum Standort von Cisco Secure Endpoint unter C:\Program Files\Cisco\AMP\version navigieren und versuchen, den Dienst manuell zu starten, wird Ihnen der Zugriff auf Berechtigungen selbst für das lokale Admin-Konto verweigert.

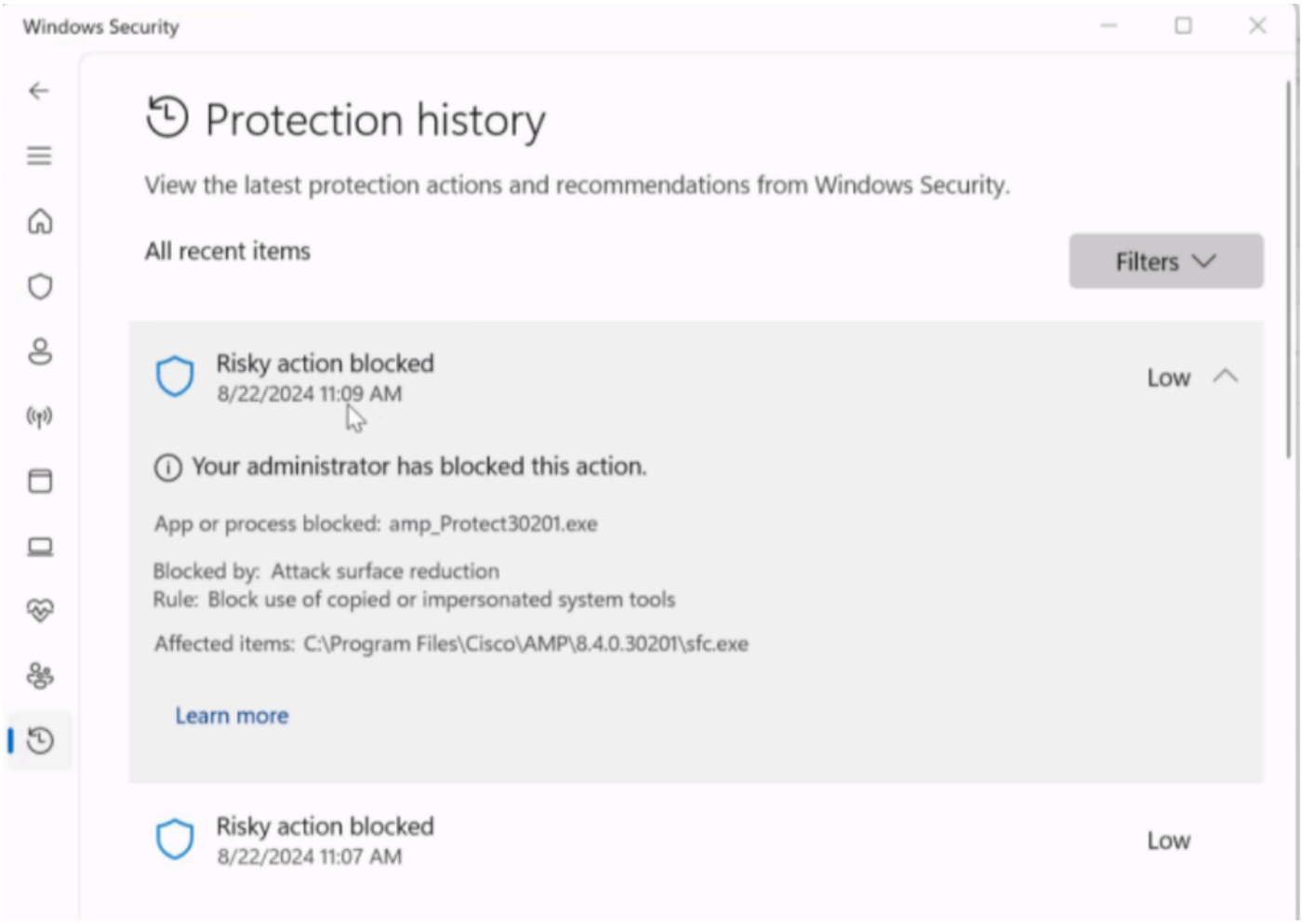


Indikator #4: Wenn wir immpro_install.log untersuchen, das Teil des Diagnosepakets ist, können wir eine ähnliche Zugangsverweigerung beobachten, die dieser Ausgabe ähnlich sieht.

```
Example #1:

(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\Pr
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\Ci
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTALL

Example #2:

(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: imn_error: fp_gen_internal: failed to open file C:\Pr
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\P
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\C
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTAL
```

Indikator #5: Wenn wir unter Windows-Sicherheit navigieren und in die Sicherheitsprotokolle einsehen, suchen Sie nach diesen Protokollmeldungen.


Protection history
View the latest protection actions and recommendations from Windows Security.
All recent items
Filters
Risky action blocked
12/09/2024 06:25
Low
Your administrator has blocked this action.
App or process blocked: powershell.exe
Blocked by: Attack surface reduction
Rule: Block use of copied or impersonated system tools
Affected items: C:\Program Files\Cisco\AMP\8.4.2.30317\sfc.exe
Learn more



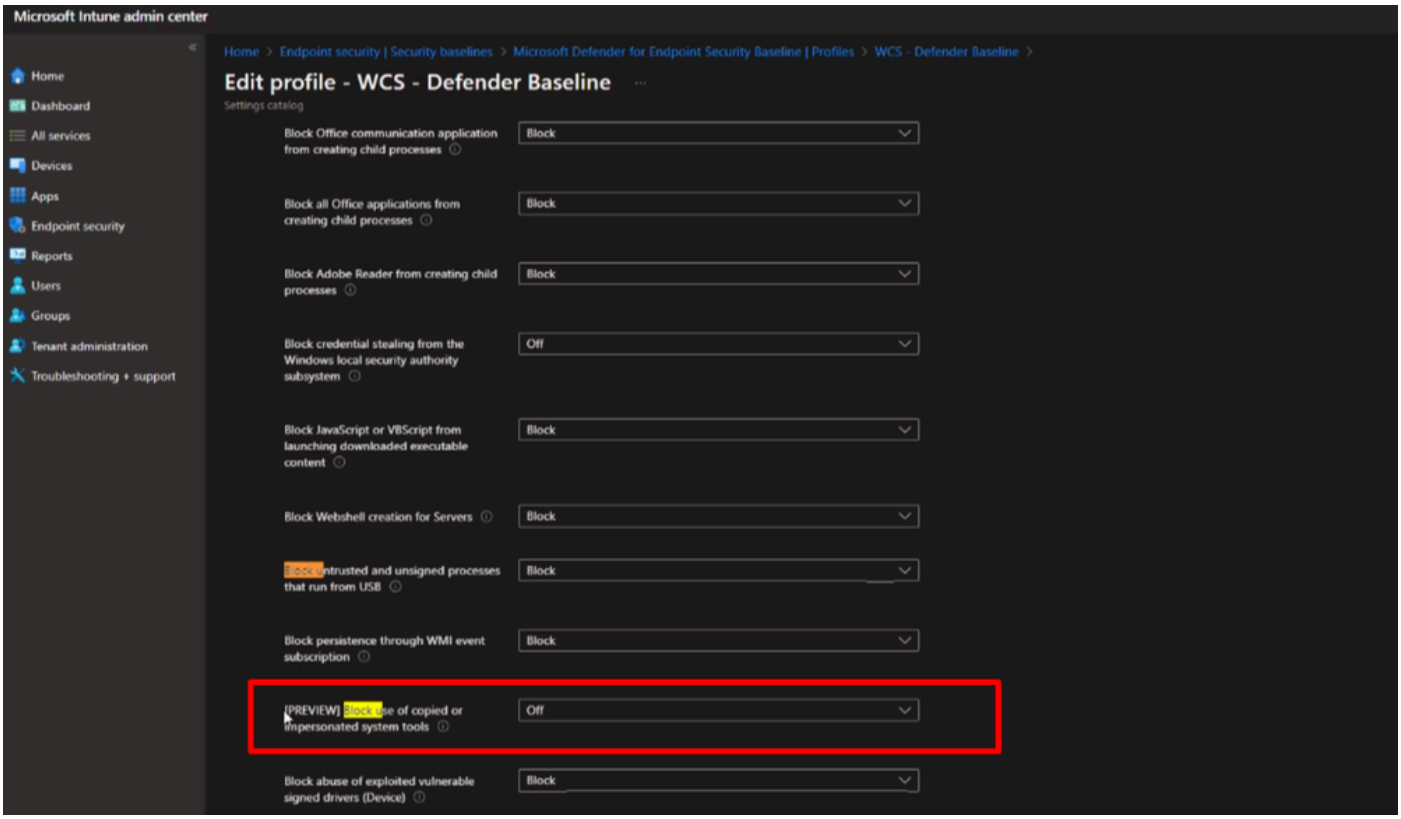
All dies deutet darauf hin, dass der sichere Endpunkt von einer Drittanbieteranwendung blockiert wird. In diesem Szenario wurde das Problem auf verwalteten Intune-Endpunkten mit entweder falsch konfigurierter oder nicht konfigurierter Reduzierung der Angriffsfläche erkannt - die Verwendung kopierter oder imitierter Systemfunktionen wird blockiert.

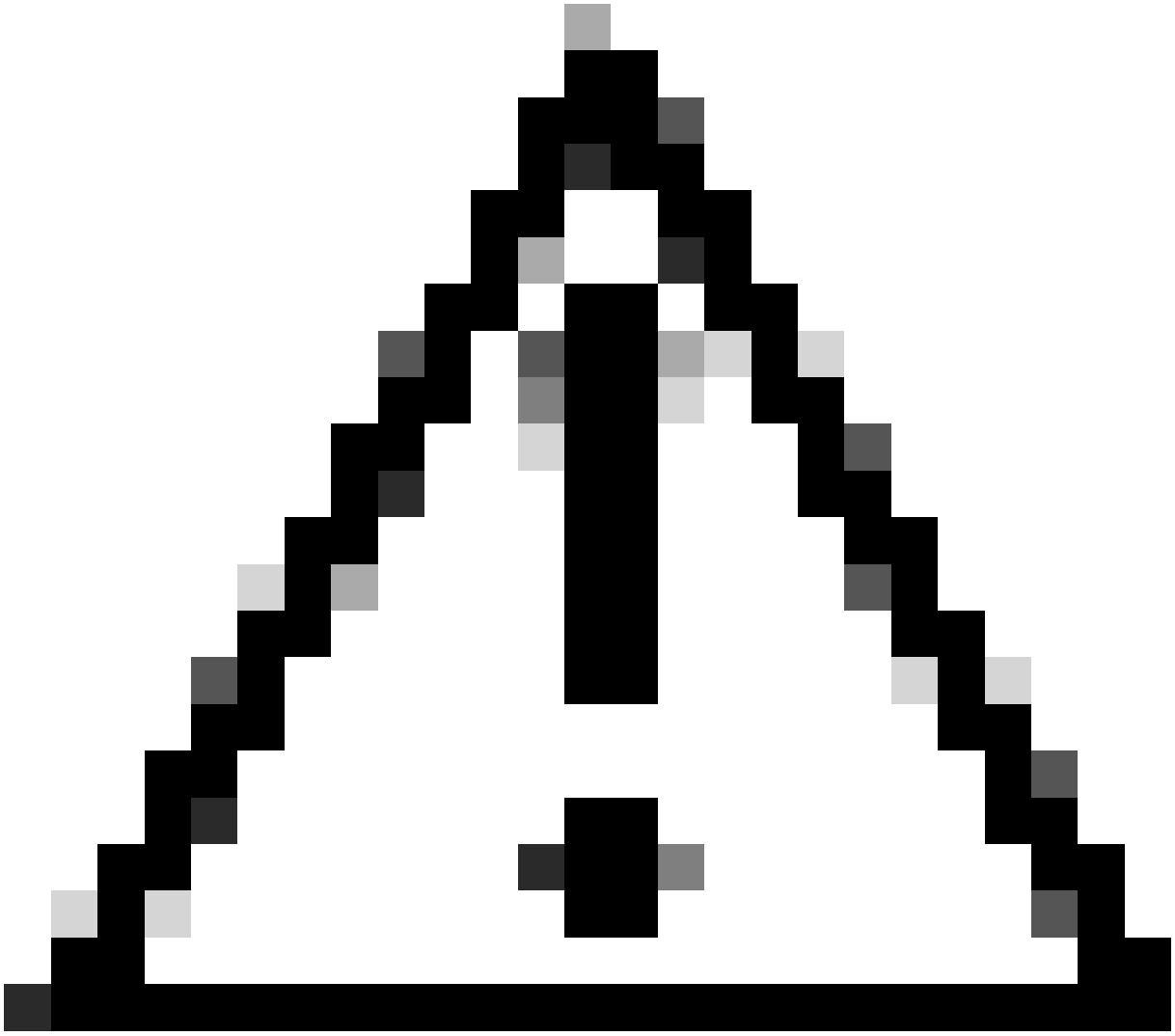
Problemumgehung

Es wird empfohlen, die Konfiguration für diese Funktion gemeinsam mit dem Anwendungsentwickler oder über diese Wissensdatenbank weiter zu konsultieren.

Zur sofortigen Problembehebung können wir entweder unser verwaltetes Endgerät in Intune in eine weniger restriktive Richtlinie verschieben oder diese Funktion vorübergehend explizit deaktivieren, bis die richtigen Schritte unternommen werden.

Dies ist die Einstellung unter dem Intune-Admin-Portal, die als temporäre Maßnahme zur Wiederherstellung der sicheren Endpunkt-Konnektivität verwendet wurde.


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Security baselines > Microsoft Defender for Endpoint Security Baseline | Profiles > WCS - Defender Baseline >
Edit profile - WCS - Defender Baseline
Settings catalog
Block Office communication application from creating child processes
Block
Block all Office applications from creating child processes
Block
Block Adobe Reader from creating child processes
Block
Block credential stealing from the Windows local security authority subsystem
Off
Block JavaScript or VBScript from launching downloaded executable content
Block
Block Webshell creation for Servers
Block
Block untrusted and unsigned processes that run from USB
Block
Block persistence through WMI event subscription
Block
(PREVIEW) Block use of copied or impersonated system tools
Off
Block abuse of exploited vulnerable signed drivers (Device)
Block



Vorsicht: Wenn Sie dieses Problem feststellen, müssen Sie die vollständige Installation aufgrund des Fehlens von sfc.exe starten.

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.