Windows-Prozess startet vor der Problemumgehung für AMP Connector - AMP für Endgeräte

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Fehlerbehebung in Advanced Malware Protection (AMP) für Endgeräte, wenn ein Windows-Prozess vor dem Systemprozessschutz (SPP) beginnt.

Mitarbeiter: Nancy Perez und Uriel Torres, Cisco TAC Engineers.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Windows-Betriebssystem
- AMP-Connector-Engines

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Windows 10-Gerät
- AMP Connector 6.2.9 Version

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Einschränkungen

Dies ist ein Fehler, der sich auf das System Process Protection-Modul auswirkt, wenn ein Prozess vor dem AMP-Anschluss CSCvo90440 beginnt.

Hintergrundinformationen

Die AMP für Endgeräte System Process Protection-Engine schützt wichtige Windows-Systemprozesse vor Speicherinjektionsangriffen anderer Prozesse.

Um SPP zu aktivieren, navigieren Sie in der AMP-Konsole zu **Management > Policies >** click *in the policy you want to change* **> Modes and Engines > System Process Protection (Verwaltung > Richtlinien >** *klicken Sie auf Edit in the policy, die Sie ändern möchten***> Modes and Engines > System Process Protection (Schutz des Systemprozesses).** Hier finden Sie drei Optionen:

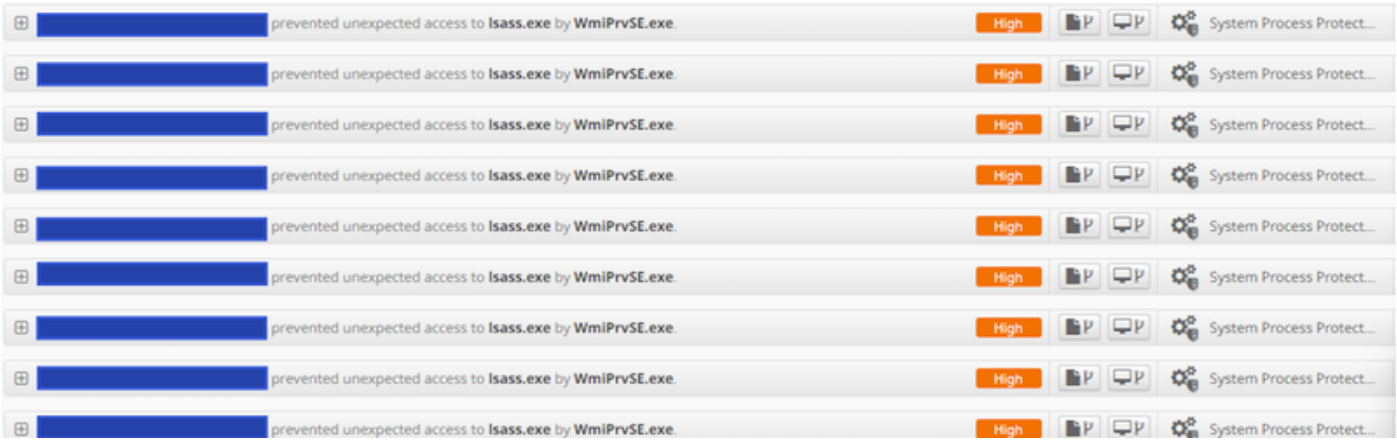
- Schutz: Blockiert Angriffe auf kritische Windows-Systemprozesse
- Audit: Benachrichtigung über Angriffe auf kritische Windows-Systemprozesse
- Deaktiviert: Der Motor ist in diesem Modus nicht aktiv.

Geschützte Systemprozesse

Die System Process Protection-Engine schützt die nächsten Prozesse:

- Session Manager-Subsystem (**smss.exe**)
- Client/Server-Laufzeitsubsystem (**csrss.exe**)
- Subsystem der lokalen Sicherheitsbehörde (**lsass.exe**)
- Windows-Anmeldeanwendung (**winlogon.exe**)
- Windows-Startanwendung (**wininit.exe**)

Wenn ein Windows-Dienst vor dem AMP-Anschluss startet (In Versionen unter 7.0.5) Systemprozessausschlüsse nicht berücksichtigt werden und selbst wenn ein Prozess ausgeschlossen ist, beendet das SPP-Modul den Prozess und ein Ereignis wird in der AMP-Konsole erstellt, wie im Bild gezeigt.



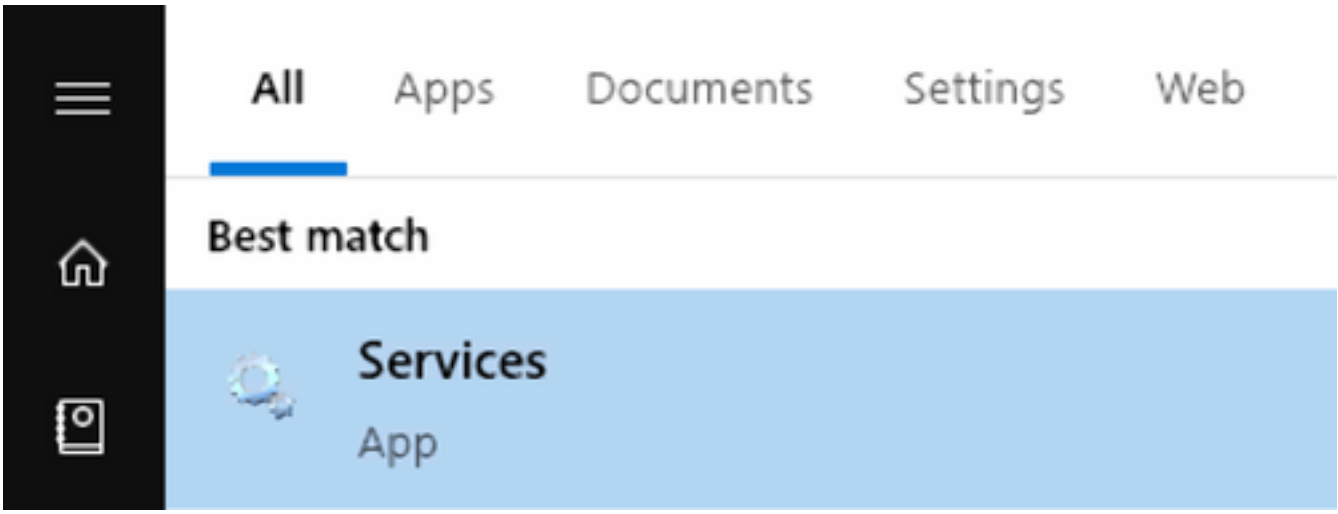
Fehlerbehebung

Die Problemumgehung dieses Fehlers besteht darin, den Windows-Dienst zu verzögern, der vor dem AMP-Dienst beginnt.

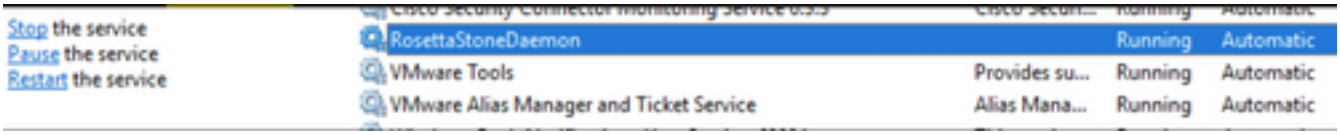
Die Anwendung Rosetta Stone wird in diesem Dokument als Beispiel genommen. Diese Anwendung wird von SPP erkannt, da sie den Prozess lsass.exe für Authentifizierungszwecke berührt.

Schritte zum Verzögern eines Windows-Diensts

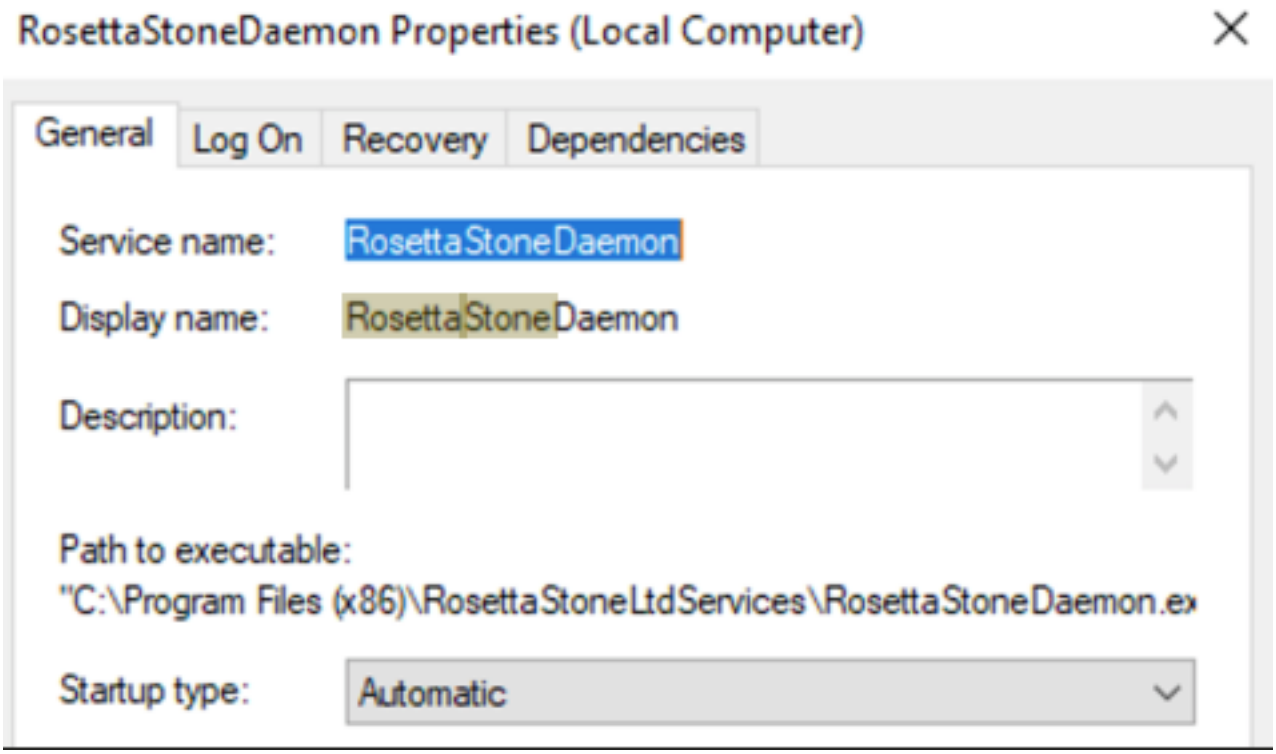
Schritt 1: Öffnen Sie services.msc, wie im Bild gezeigt.



Schritt 2: Finden Sie den Rosetta Stone-Dienst.

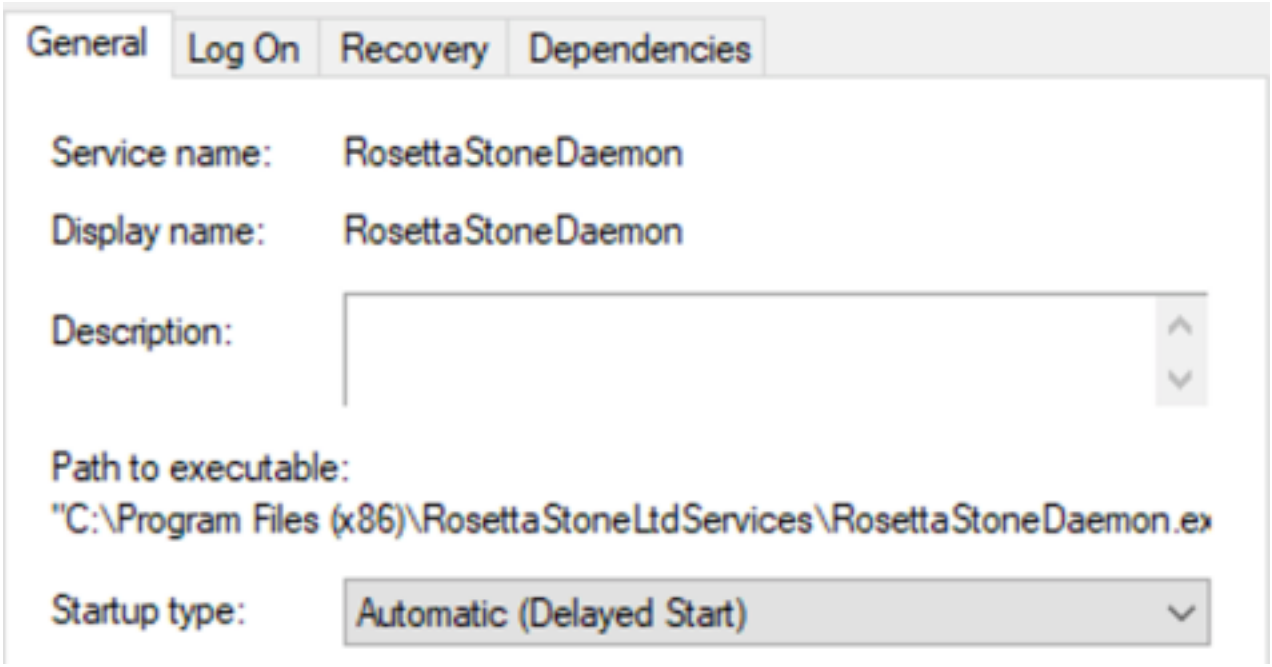


Schritt 3: Klicken Sie mit der rechten Maustaste auf RosettaStoneDaemon und dann auf Eigenschaften.



Der Starttyp wird standardmäßig als Automatisch konfiguriert, d. h., RossettaStoneDaemon startet automatisch im Startvorgang.

Schritt 4: Klicken Sie auf das Dropdown-Menü, und wählen Sie Automatisch (Verzögerter Start) aus.



Diese Konfiguration verhindert, dass der RosettaStoneDaemon-Dienst vor dem AMP-Anschluss gestartet wird.

Schritt 5: Klicken Sie auf Übernehmen.

Verzögerung des Prozesses mit der Befehlszeile

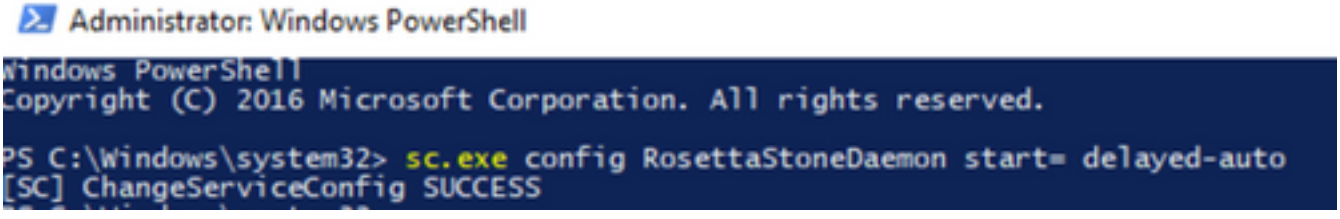
Für PowerShell/CMD können die nächsten Befehle verwendet werden.

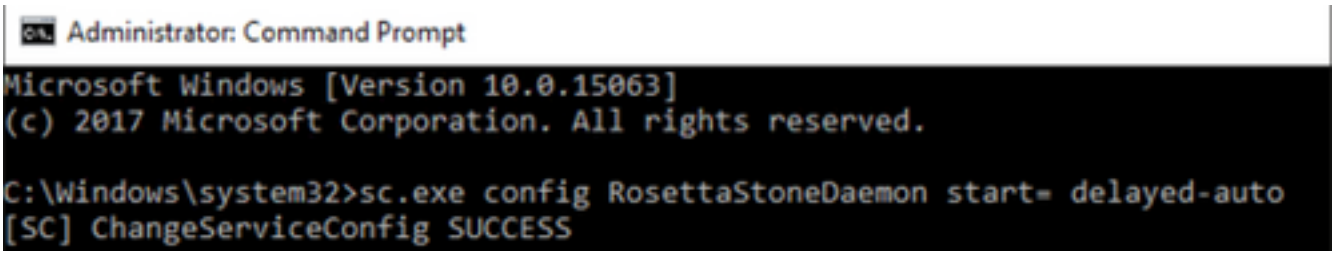
Schritt 1: Führen Sie PowerShell/CMD als Administrator aus.

Schritt 2: Führen Sie diesen Befehl aus:

```
sc.exe config RosettaStoneDaemon start= delayed-auto
```

Hinweis: Rosetta Stone = RosettaStoneDaemon.





In diesem Abschnitt können Sie den Anwendungsnamen RosettaStoneDaemon für den Prozess ersetzen, den Sie verzögern möchten.

> **Vorsicht**: Connector Version 7.0.5 und weiter implementieren bereits eine Lösung für diesen Fehler. Diese Problemumgehung ist für Anschlussversionen unter 7.0.5 vorgesehen.