

Windows进程在AMP连接器解决方案之前启动 — 面向终端的AMP

目录

[简介](#)

[要求](#)

[使用的组件](#)

[限制](#)

[背景信息](#)

[故障排除](#)

[延迟Windows服务的步骤](#)

[使用命令行延迟进程](#)

简介

本文档介绍在系统进程保护(SPP)之前启动Windows进程时，在面向终端的高级恶意软件防护(AMP)中进行故障排除的步骤。

作者：Nancy Perez和Uriel Torres，思科TAC工程师。

要求

Cisco 建议您了解以下主题：

- Windows操作系统
- AMP连接器的引擎

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows 10设备
- AMP连接器6.2.9版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

限制

当AMP连接器CSCvo90440之前的进程启动时，这是一个影响系统进程保护引擎的[错误](#)。

背景信息

面向终端的AMP系统进程保护引擎可保护关键Windows系统进程免受其他进程的内存注入攻击。

要启用SPP，请在AMP控制台上导航至**Management > Policies >**，单击要修改的策略中的**Edit > Modes and Engines > System Process Protection**，您可以在**此**找到三个选项：

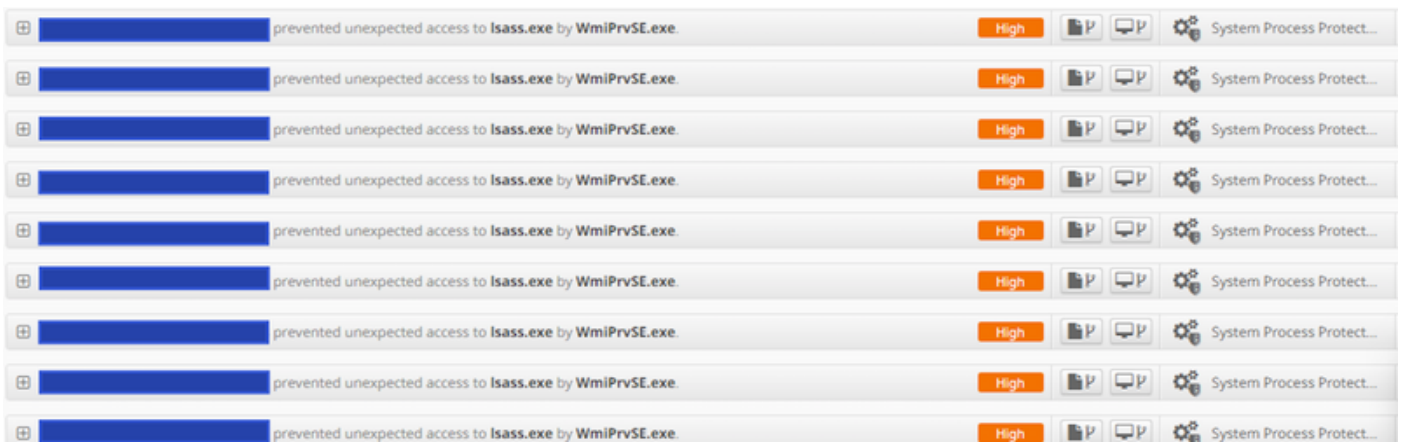
- 保护：阻止对关键Windows系统进程的攻击
- 审核：通知对关键Windows系统进程的攻击
- 禁用:此模式下引擎未激活

受保护的系统进程

系统进程保护引擎可保护下一个进程：

- 会话管理器子系统(**smss.exe**)
- 客户端/服务器运行时子系统(**csrss.exe**)
- 本地安全机构子系统(**lsass.exe**)
- Windows登录应用程序(**winlogon.exe**)
- Windows启动应用程序(**wininit.exe**)

当Windows服务在AMP连接器（在7.0.5以下版本中）系统进程排除之前启动时，即使排除了进程，SPP引擎也会停止该进程并在AMP控制台中创建事件，如图所示。



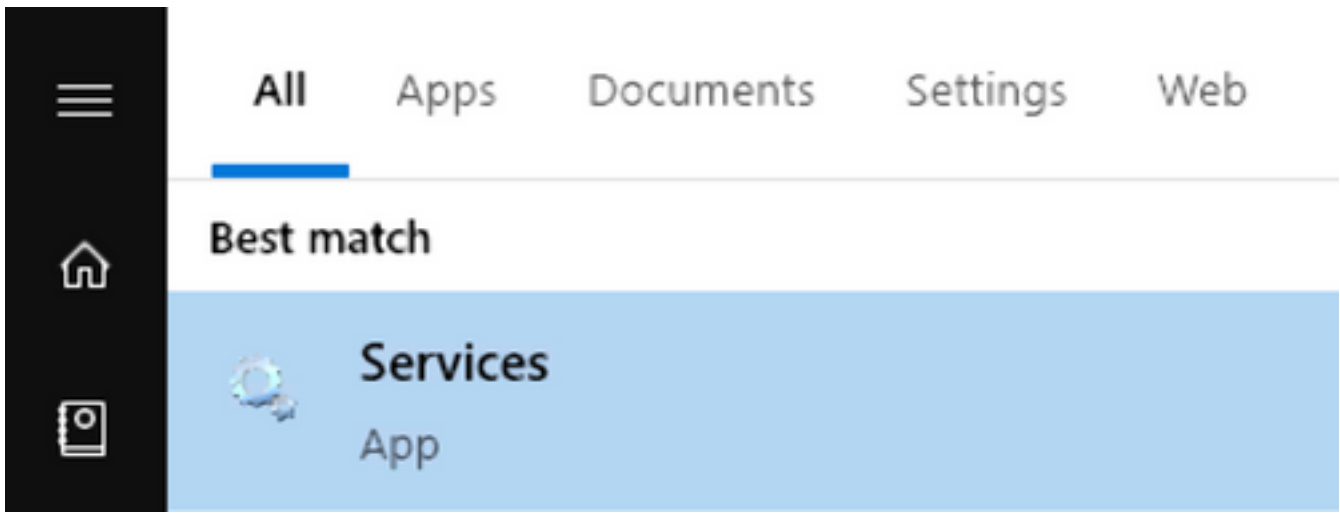
故障排除

此Bug的解决方法是延迟在AMP服务之前启动的Windows服务。

Rosetta Stone应用程序在本文档中作为示例。SPP检测到此应用，因为它为了进行身份验证而与lsass.exe进程接触。

延迟Windows服务的步骤

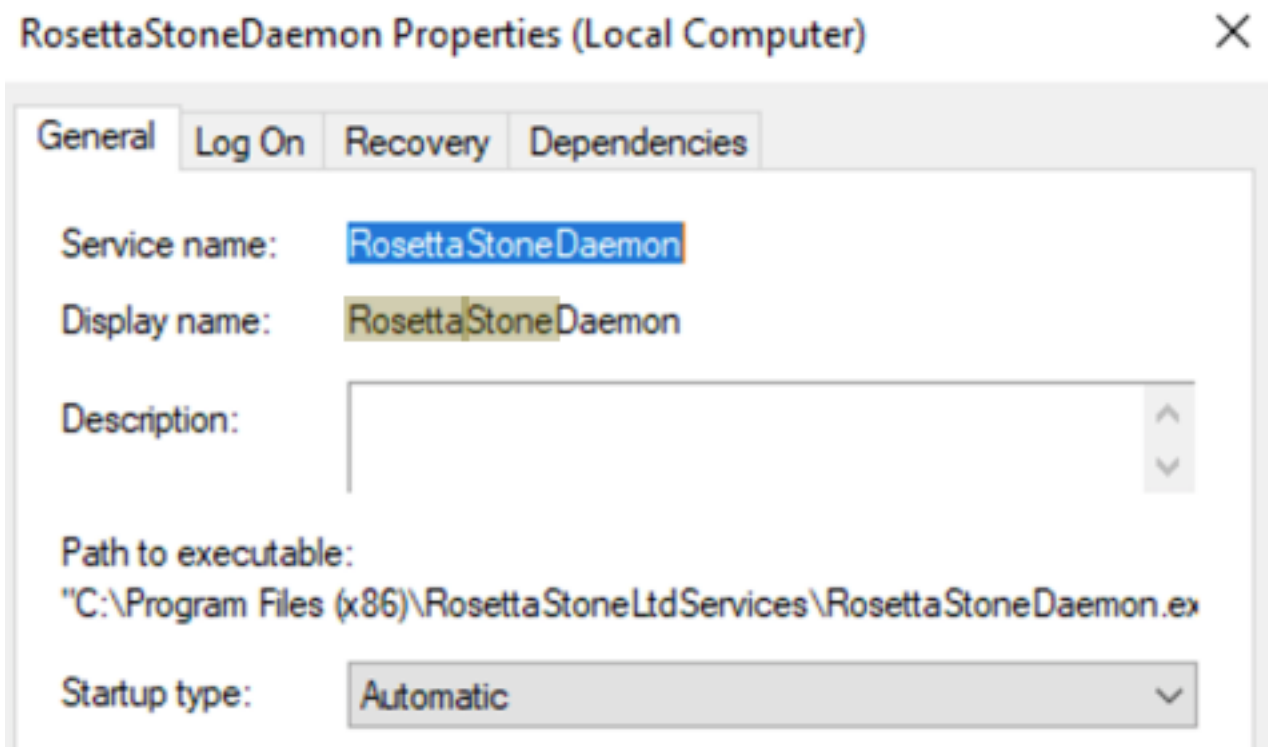
步骤1.打开services.msc，如图所示。



步骤2. 查找Rosetta Stone服务。

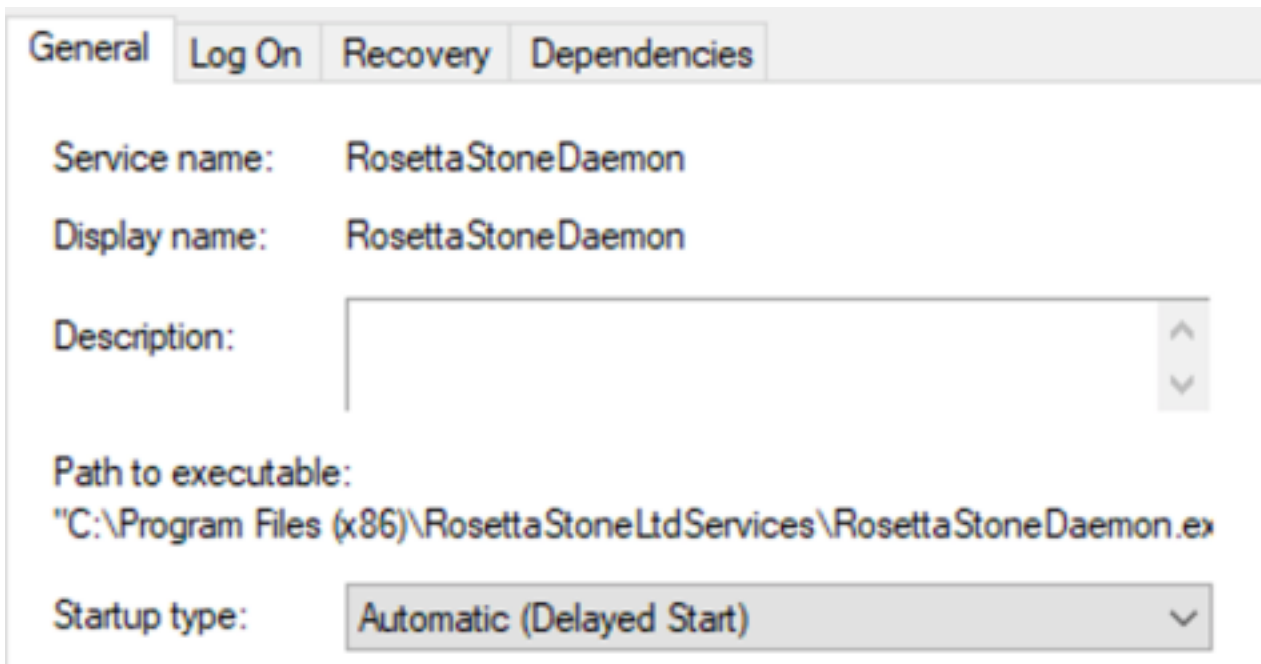
Service Name	Description	Status	Startup Type
Cisco Security Connector monitoring Service 0.3.3	Cisco Secur...	Running	Automatic
RosettaStoneDaemon		Running	Automatic
VMware Tools	Provides su...	Running	Automatic
VMware Alias Manager and Ticket Service	Alias Mana...	Running	Automatic

步骤3. 右键单击RosettaStoneDaemon，然后单击“属性”。



默认情况下，启动类型配置为自动，这意味着RosettaStoneDaemon在引导过程中自动启动。

步骤4. 点击下拉菜单并选择自动（延迟开始）。



此配置会阻止在AMP连接器之前启动RosettaStoneDaemon服务。

步骤5. 点击Apply。



使用命令行延迟进程

对于PowerShell/CMD，可以使用下一个命令。

步骤1. 以管理员身份执行PowerShell/CMD。

步骤2. 执行以下命令：

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

注意：Rosetta Stone = RosettaStoneDaemon。

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> sc.exe config RosettaStoneDaemon start= delayed-auto
[SC] ChangeServiceConfig SUCCESS
```

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc.exe config RosettaStoneDaemon start= delayed-auto
[SC] ChangeServiceConfig SUCCESS
```

在本节中，您可以替换要延迟的进程的RosettaStoneDaemon应用程序名称。

注意：连接器版本7.0.5及以后已经针对此漏洞实施了解决方案。此解决方法适用于7.0.5以下的连接器版本。