How to Fix the CrowdStrike Falcon BSOD Issue on a Windows 10 Virtual Machine

Ryan Boulrice

7/20/2024

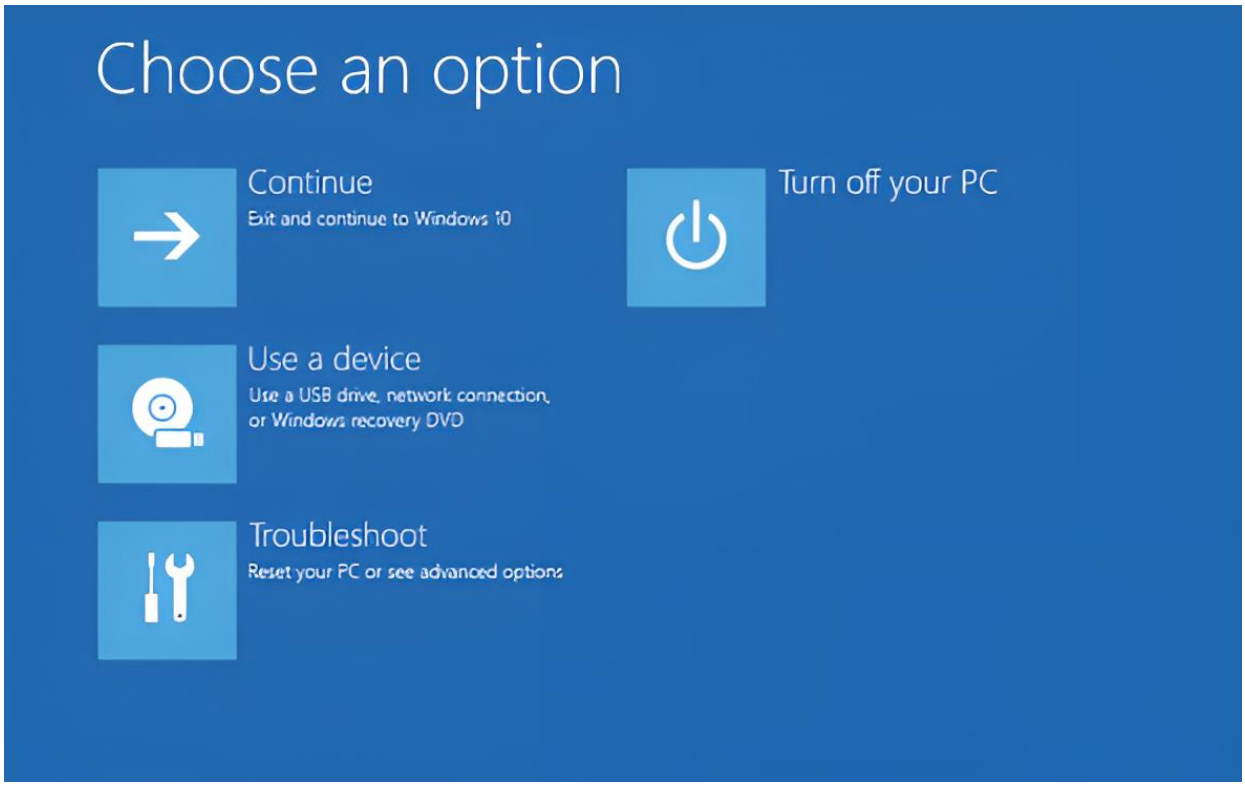
Summary

To resolve the BSOD issue caused by a faulty CrowdStrike Falcon Sensor update, we must boot the Windows 10 VM into Safe Mode using the Windows Recovery Environment (WinRE). After force-shutting down the VM three times to access WinRE, we need to open the Command Prompt with administrative privileges. We then navigate to C:\Windows\System32\drivers\CrowdStrike and delete the C-00000291*.sys file to prevent the faulty driver from loading. This procedure will allow the VM to boot normally without encountering the BSOD error. The steps for this process are outlined in the following documentation.

,

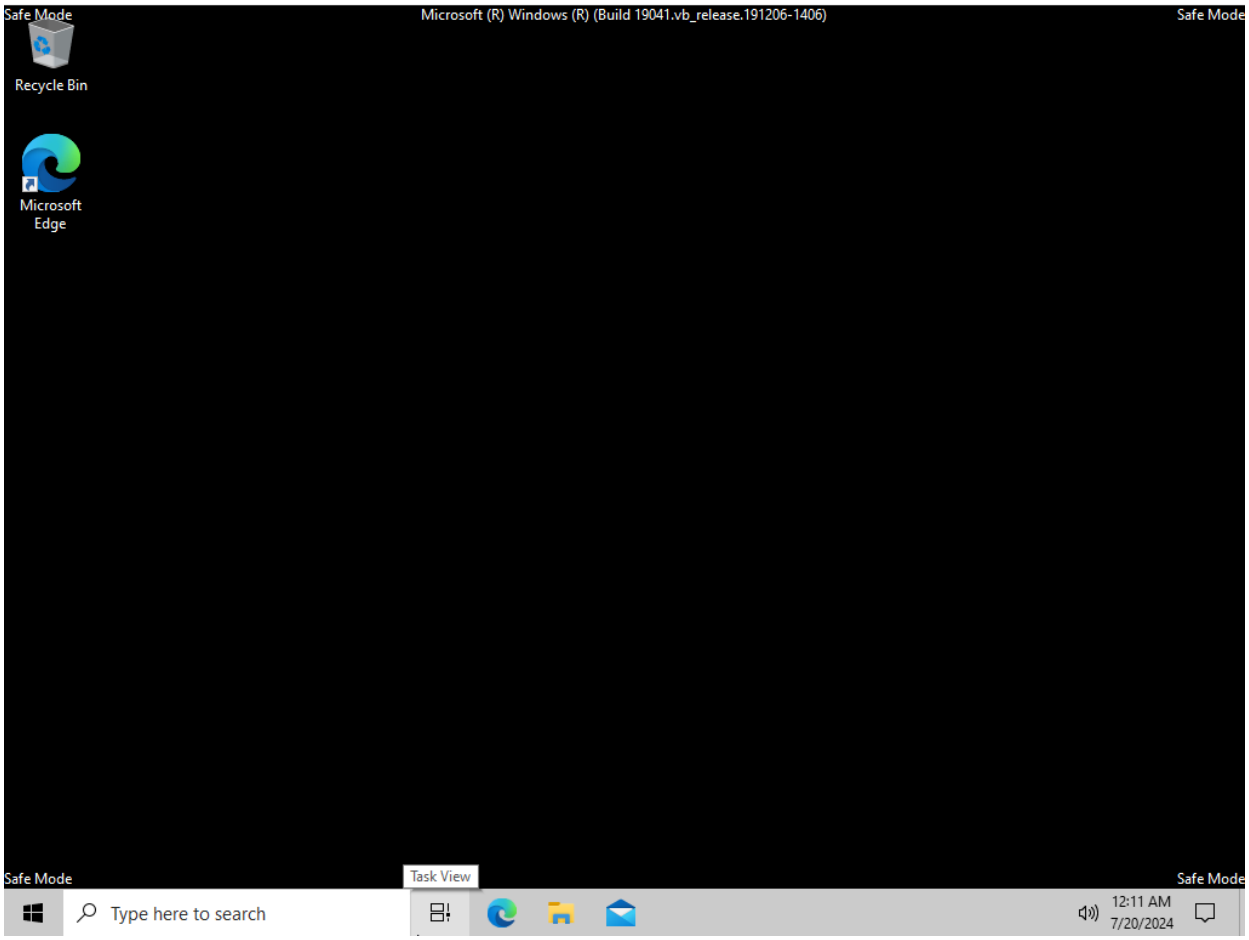
Boot Into Safe Mode through WinRE

The first step in fixing the blue screen of death caused by CrowdStrike's faulty update is to boot your Windows VM into Safe Mode. To do this, restart your VM and wait for the blue screen to appear. Force-shutdown your VM by either closing the VM window or using your choice of hypervisor's power off button. Repeat this process 3 times. On the third restart, Windows should automatically enter the Windows Recovery Environment, or WinRE.



The Windows Recovery Environment

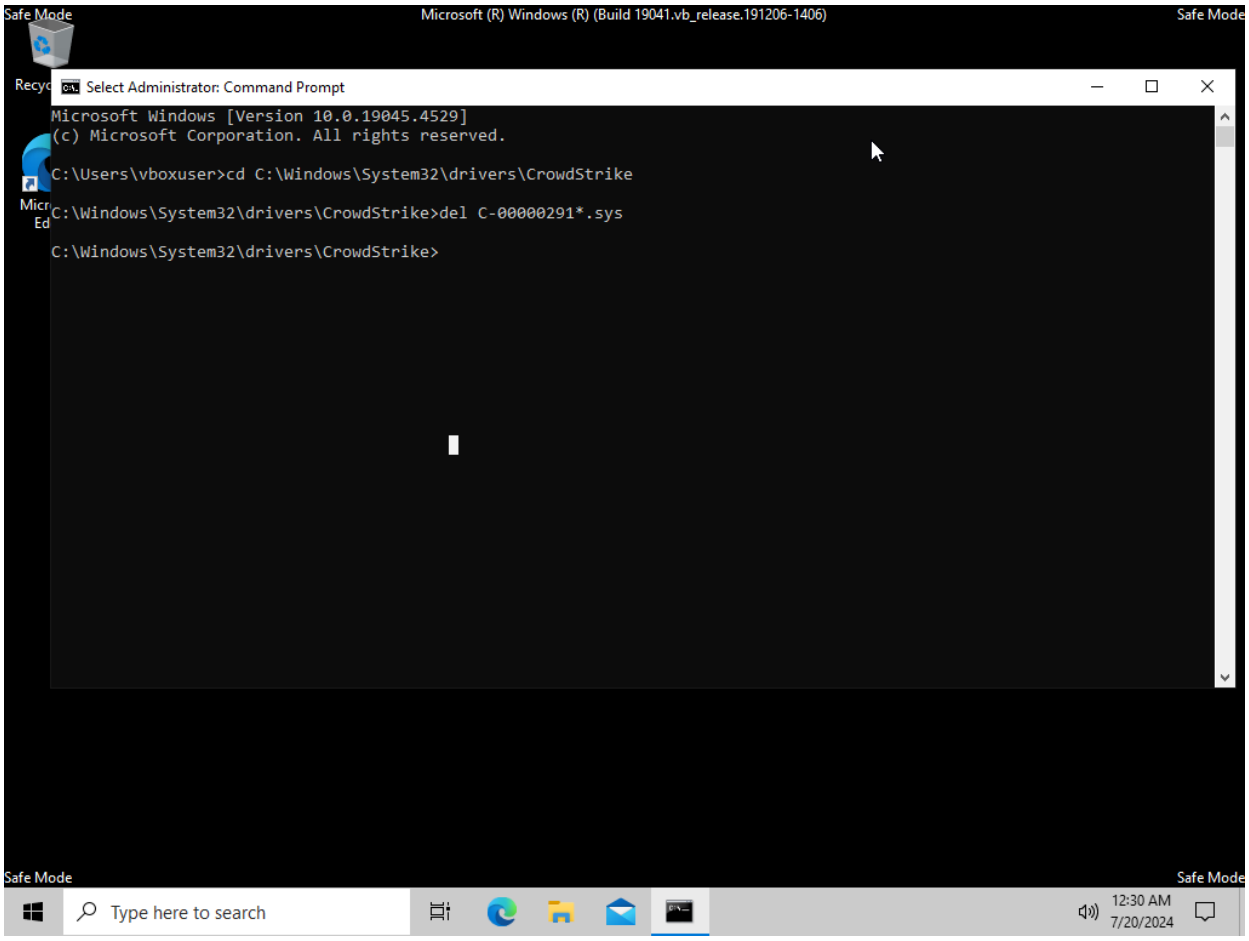
Within WinRE, select Troubleshoot, then Advanced Options, Startup Settings, then restart. After the VM restarts, you should see a list of options. Press F4 or alternatively 4 to start Windows 10 in Safe Mode.



Windows 10's Safe Mode

Locate and Delete C-00000291.sys

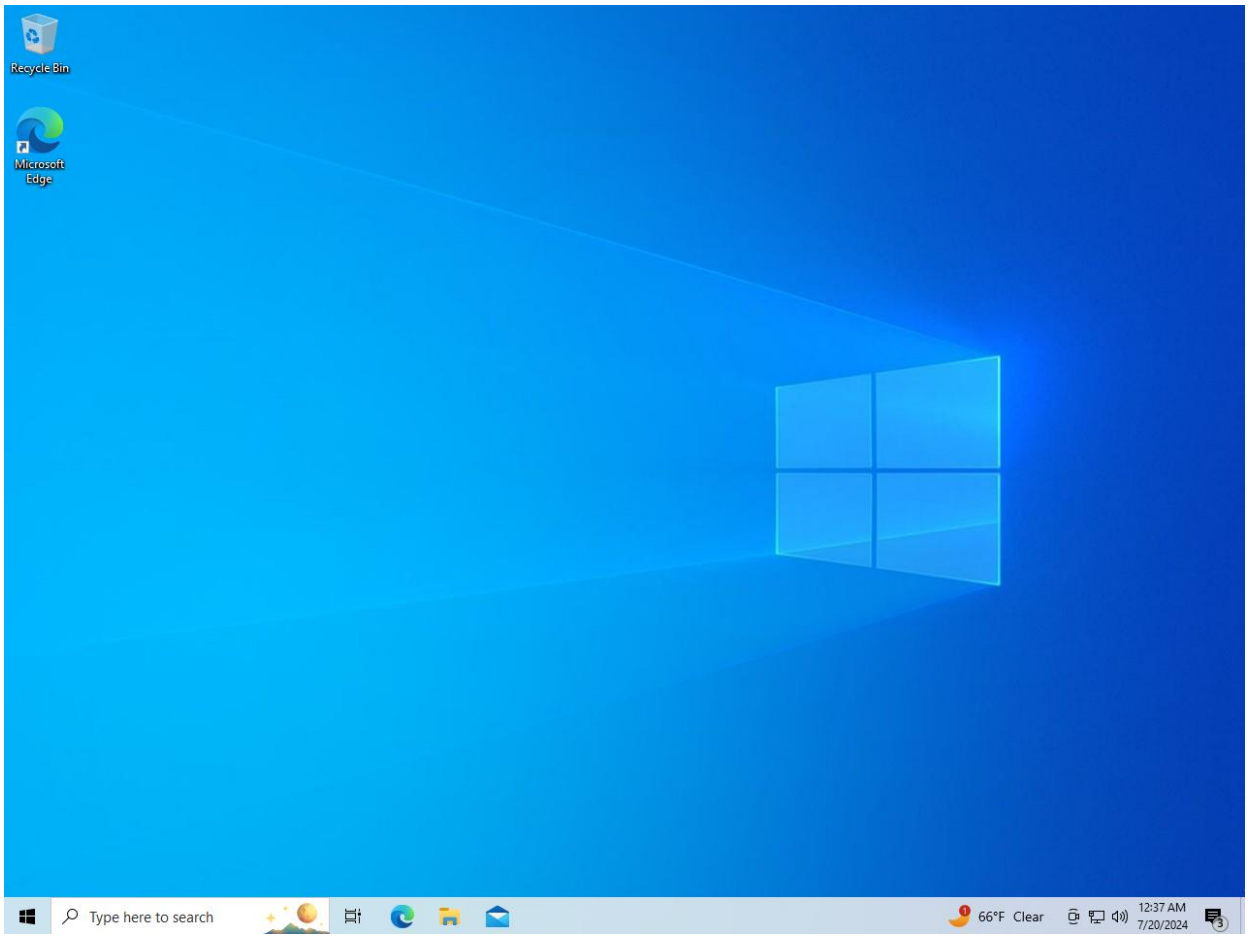
Start up a command prompt by typing “cmd” into the Windows Search bar, make sure you are running it as an administrator. Use the command “cd C:\Windows\System32\drivers\CrowdStrike” to navigate to the relevant directory, and run the command “del C-00000291*.sys” to delete the file. This allows us to be able to boot into an environment where third-party drivers like CrowdStrike’s driver are not able to load, negating the BSOD issue.



The two commands required to mitigate the issue, successfully executed

Boot the Host

After performing these commands, you should be able to boot the Windows 10 VM regularly, without the BSOD issue occurring. For more information on the CrowdStrike vulnerability and other possible mitigations, refer to our writeup on the subject.



The successfully booted Windows 10 VM