(https://www.crowdstrike.com/)

Using the Microsoft Recovery Tool for Automated Host Remediation

Published Date: Jul 21, 2024

Applies To

Hosts impacted by the Content Update issue (/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19)

Procedure

Microsoft, in partnership with CrowdStrike, have released a utility to assist with recovering hosts impacted by the Content Update issue (/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19). This Microsoft signed utility enables IT Admins to create a bootable USB Drive for automated remediation including BitLocker Recovery Key support.

Requirements:

- A Windows 64-bit client with at least 8GB of free space from which the tool can be run to create the bootable USB drive.
- Administrative privileges on the Windows client from prerequisite #1.
- USB drive with (1GB). All existing data on this USB will be wiped.
- A BitLocker recovery key for each BitLocker-enabled impacted device on which the generated USB device will be used.

Procedure

1. Download the utility from Microsoft here (https://go.microsoft.com/fwlink/?linkid=2280386)
2. Extract the utility to a working directory
3. Open PowerShell as an administrator and navigate to your working directory
4. Run the MsftRecoveryToolForCS.ps1 file
5. Please wait a few minutes as the utility begins initial Windows PE image creation, including downloading required files from Microsoft
6. The utility will prompt you to select an option for adding drivers to the WinPE image. Press Y only if you need to add drivers to support specific host hardware. Otherwise, select N to just use the base WinPE drivers.
   a. If you selected Y, enter the path where you have stored INF based drivers and the utility will add them to the WinPE image.
7. When prompted, insert a USB Drive and provide the drive letter it is assigned by Windows
8. Once creation is completed, you can remove the USB Drive from the device.
9. Insert the USB Flash Drive into the target system
10. Reboot the target system and enter the UEFI boot Menu (usually F1, F2, F8, F11, or F12).
11. Select the USB Drive from the Boot Menu. If given both a MBR and UEFI option, select UEFI
12. Wait for Windows PE to load
13. If prompted, enter your BitLocker Recovery Key to unlock the volume
14. Let the utility find and remove the impacted Channel File 291 sys file
15. The utility will report once it's completed and exit Windows PE, which should then reboot the targeted system.
16. The targeted system should now load Windows successfully.