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

Building CrowdStrike Bootable Recovery ISOs

Published Date: Jul 22, 2024

Objective

This guide shows you how to build your own bootable image files to automate the recovery of Windows hosts affected by the recent Falcon Content Update.

Procedure

There are two bootable image types available. Use the ISO image that best suits your needs.

1. **CSPERecovery** - This image uses Windows PE to remove the impacted Channel File 291 with minimal user interaction
    a. If the volume has BitLocker Encryption, the bootable image will prompt for the BitLocker Recovery Key before performing the automated remediation
2. **CSSafeBoot** - This image uses Windows PE to reboot the host into *Safe Mode with Networking* to allow manual removal of Channel File 291 using Windows Explorer or Command Prompt
    a. If the volume has BitLocker Encryption, **the Recovery Key is not required**
    b. Useful for systems having difficulty entering Safe Mode

Creating Bootable Images

The following procedure will produce two bootable ISO images using the latest Microsoft ADK and Windows PE add-ons and drivers, along with common storage and input drivers for enterprise storage controllers including VirtIO, Intel RAID, HP and Dell storage controllers, VMware accelerated virtual storage, etc. These ISO images will also include the Falcon Windows Sensor host recovery scripts. Note - This script may take upwards of 20 minutes to complete.

Requirements

- A Windows 10 (or higher) 64-bit client with at least 8GB of free space, and administrative privileges

Procedure

Default (CrowdStrike-recommended drivers)

Builds two bootable ISO images with device drivers from Redhat/Virtio, Dell, HP and VMWare

1. Download the falcon-windows-host-recovery (https://github.com/CrowdStrike/falcon-windows-host-recovery) project from the CrowdStrike github (https://github.com/CrowdStrike)
    a. Click the green *Code* button and select *Download ZIP*
2. Extract *falcon-windows-host-recovery-main.zip* file contents to a directory of your choosing
    a. Example: `C:\falcon-windows-host-recovery`
3. Open a Windows PowerShell command prompt
    a. Type `powershell` in taskbar Search
    b. Right click on *Windows PowerShell*, and select *Run as administrator*
    c. In PowerShell Command Prompt
        i. Change into your extracted file directory
        `cd C:\falcon-windows-host-recovery`

4. Create the **CSPERecovery** and **CSSafeBoot** bootable ISO images
   a. `Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process`
   b. `.\BuildISO.ps1` - downloads device drivers and creates ISO images
5. Build output
   a. `C:\falcon-windows-host-recovery\CSPERecovery_x64.iso`
   b. `C:\falcon-windows-host-recovery\CSSafeBoot_x64.iso`

WinPE Drivers and Custom-supplied Drivers

Builds two bootable ISO images with only WinPE drivers, or with WinPE and drivers you prefer

1. Open a Windows PowerShell command prompt
   a. Change into your extracted file directory
   `cd C:\falcon-windows-host-recovery`
2. If you wish to include any custom drivers, download and unpack device drivers of your choosing into `C:\falcon-windows-host-recovery\Drivers`
3. Create bootable ISO images with your preferred drivers
   a. `Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process`
   b. `.\BuildISO.ps1` -SkipThirdPartyDriverDownloads
4. Build output
   a. `C:\falcon-windows-host-recovery\CSPERecovery_x64.iso`
   b. `C:\falcon-windows-host-recovery\CSSafeBoot_x64.iso`

Writing ISO files to a USB stick and booting off of it

1. Download Rufus, an open-source utility for creating bootable USB sticks from https://rufus.ie/en/ (https://rufus.ie/en/)
2. Open Rufus:
   a. Select the desired USB Flash Drive target using the “Device” dropdown menu (NOTE: this USB Flash Drive will be wiped clean, make sure it’s the correct one)
   b. Select the either the CSPERecovery or CSSafeBoot ISO file using the SELECT button beside “Boot Selection” label
   c. Select “GPT” for the using the “Partition scheme” dropdown menu
   d. Select “UEFI (non CSM)” using the “Target System” dropdown menu
   e. Press Start
   f. If prompted to write in ISO mode or ESP mode, select ESP Mode. ESP mode is more likely to be compatible with older hardware.
3. Once complete, connect the USB Flash Drive to the intended target system
4. Confirm that the target host has network access, preferably via wired ethernet
5. Reboot the target system and enter the UEFI boot Menu (usually F1, F2, F8, F11, or F12)
6. Prepare to select the USB Flash Drive. If given both a MBR and UEFI option with the same label, prepare to select UEFI
7. Wait while Windows PE loads and follow next sections for Running CSSafeBoot or CSPERecovery respectively

Running CSSafeBoot

1. CSSafeBoot will automatically reconfigure the bootloader on the machine to boot into Safe Mode with Networking and reboot
2. If your system reboots into the Windows Recovery environment as a part of a prior boot loop, select Continue. The machine will reboot into safe mode on the next boot.
3. Log in as an user with Local Administrator permissions
4. Confirm the Safe mode banner is displayed on the desktop

5. Open Windows Explorer and navigate to `C:\Windows\System32\drivers\Crowdstrike`
6. Delete all offending files that start with C-00000291*
7. Open command prompt (Right click -> Run as administrator)
8. Type bcdedit /deletevalue {default} safeboot, then press Enter
9. Reboot the device and verify the operating system loads successfully

Running CSPERecovery

1. If more than one drive is detected, select the drive letter associated with the impacted OS
2. If prompted, enter your BitLocker Recovery Key to unlock the volume
3. Let the utility find and remove the impacted Channel File 291 sys file
4. The utility will reboot the device and the operating system should load successfully

PXE Booting

For PXE booting, these ISO files can be deployed and booted through existing PXE booting capability deployed in your organization. Due to significant differences in network and software configurations with PXE booting, we cannot recommend specific generic PXE booting instructions.