Building CrowdStrike Bootable Recovery Images

Solution:
Sensors - Windows OS Platforms
Published Date: Jul 26, 2024

Objective

Build bootable images to remediate Windows hosts impacted by the recent Falcon Content Update.

Watch CrowdStrike Host Remediation with Bootable USB Drive video for a demonstration.

What's New

Release 1.3.1

- **CSPERecovery**: Removes prompt to accept CrowdStrike signing certificate during remediation
- **CSPERecovery:** Disables safeboot after successful remediation, allowing Windows to boot normally

Features

- **Build Tools**
  - Default - Image with Device Drivers
  - Optional - Image with Custom Drivers: minimal, limited and custom (user defined)
  - Optional - Image with Custom BitLocker Recovery support via CSV
- **BitLocker Tools**
  - Optional - Create CSV of BitLocker Recovery Keys from Active Directory/Entra ID
- **Host Remediation Tools**
  Two bootable images are available - use the image that best suits your needs.
  - *CSSafeBoot* - automated and manual host remediation for Windows
  - *CSPERecovery* - automated host remediation with manual or automatic BitLocker Recovery Keys

Procedure

Build Tools

Use this project to build bootable Windows PE images using the latest Microsoft ADK, Windows PE add-ons, drivers, and CrowdStrike's remediation scripts.

Requirements

- A Windows 10 (or higher) 64-bit client with at least 16GB of free space, and administrative privileges.

1. Download the falcon-windows-host-recovery github project as a ZIP file.
    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-main`
    b. IMPORTANT: *path cannot contain spaces or special characters*

Default - Image with Device Drivers

Build bootable images with device drivers for all the following:

Red Hat/VirtIO VMs, Dell systems, HP systems, VMWare VMs, Microsoft Surface devices (Pro 8, 9, 10, Laptop 4 (Intel/AMD), 5, 6), common AMD SATA controllers, and common Intel / LSI MegaSAS RAID cards.

NOTE: may take upwards of 30 minutes to build based on network and disk performance

1. Open a Windows PowerShell command prompt (as Administrator), set execution policy and build images
    a. `cd C:\falcon-windows-host-recovery-main`
    b. `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`
    c. `.\BuildISO.ps1` - downloads default set of device drivers and creates ISO images
2. Optional Command-line Arguments for *BuildISO.ps1* script
    a. `-SkipBootPrompt` - Disable the `press any key to boot from [media]` prompt when the system boots
        i. This feature may not work on all systems
3. Output: images
    a. `C:\falcon-windows-host-recovery-main\CSPERecovery_x64.iso`
    b. `C:\falcon-windows-host-recovery-main\CSSafeBoot_x64.iso`

Optional - Image with Custom Device Drivers

Build bootable images with minimal drivers only, a limited set of drivers, or with your own custom device drivers.

1. Open a Windows PowerShell command prompt (as Administrator)
    a. `cd C:\falcon-windows-host-recovery-main`
2. Custom drivers - download and unpack device drivers into
    a. `C:\falcon-windows-host-recovery-main\Drivers`
    b. NOTE: drivers in *\Drivers will always be installed*, regardless of command-line arguments.

3. Command-line Arguments for `BuildISO.ps1` script
    a. Optional drivers - include one or more driver sets (any combination supported)
        i. `-IncludeCommonDrivers` - most common CrowdStrike customer device drivers
        ii. `-IncludeDellDrivers`
        iii. `-IncludeHPDrivers`
        iv. `-IncludeSurfaceDrivers`
        v. `-IncludeVMwareDrivers`
    b. Minimal drivers - skip all included driver sets (NOTE: overrides any `-Include* args`)
        i. `-SkipThirdPartyDriverDownloads`
4. Build bootable images
    a. `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`
    b. `.\BuildISO.ps1 <Command-line Arguments>`
5. Output: images
    a. `C:\falcon-windows-host-recovery-main\CSPERecovery_x64.iso`
    b. `C:\falcon-windows-host-recovery-main\CSSafeBoot_x64.iso`

Optional - Image with Custom BitLockerKeys.csv

Build bootable images with BitLocker Recovery Keys in the *CSPERecovery*

⚠️ **WARNING: BitLocker Recovery Keys should be rotated after host remediation**

BitLocker Keys via CSV Example of your Recovery Keys in a CSV file

- IMPORTANT: column headers KeyID and RecoveryKey are required and case sensitive

KeyID	**RecoveryKey**
3ca7495e-4252-432b-baf1-SAMPLE	001317-088010-034473-667247-160608-471717-100894-INVALID
92e89e08-ad6e-4a98-e584-SAMPLE	509542-050497-158529-325316-496853-372340-593355-INVALID
72E460C8-4FE8-4249-99CF-SAMPLE	529408-021370-702581-530739-028721-610907-461582-INVALID

1. Open a Windows PowerShell command prompt
    a. Change into your extracted file directory
        i. `cd C:\falcon-windows-host-recovery-main`
2. Include BitLocker Recovery Keys - via CSV file named *BitLockerKeys.csv*

    a. `C:\falcon-windows-host-recovery-main\BitLockerKeys.csv`
    b. IMPORTANT: see *Best Practices* section below for safe handling and destruction of BitLocker Recovery Keys
3. Create bootable images
    a. `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`
    b. `.\BuildISO.ps1 <Command-line Arguments>`
4. Output: images
    a. `C:\falcon-windows-host-recovery-main\CSPERecovery_x64.iso`
    b. `C:\falcon-windows-host-recovery-main\CSSafeBoot_x64.iso`

BitLocker Tools

Requirements

- Powershell 7 or higher
- Server Manager -> Local Server: *disable* **IE Enhanced Security Configuration**
- Active Directory export requires a Domain Administrator user on a domain-joined Windows Server OS
- Entra ID export script requires connectivity to Microsoft Graph, and a cloud user with OAuth scopes *BitLockerKey.ReadBasic.All* and *Device.Read.All*

Optional - Automated BitLocker Recovery Key Export from Active Directory or Entra ID

Generates a *BitLockerKeys.csv* via automated export of BitLocker Recovery Keys

1. Open a Windows PowerShell command prompt (as Administrator)
    a. Change into your extracted file directory
        i. `cd C:\falcon-windows-host-recovery-main`
2. Command-line Arguments for *Export-BitLockerRecoveryKeys.ps1* script
    a. `-ActiveDirectory` - extract BitLocker keys from Active Directory
    b. `-ActiveDirectory -OU` - extract BitLocker keys for specific Organizational Unit
    c. `-EntraID` - extract BitLocker keys from Entra ID
    d. `-ActiveDirectory -EntraID` - extract BitLocker keys from both Active Directory and Entra ID
3. Extract BitLocker Recovery keys from source
    a. `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`
    b. `.\Export-BitLockerRecoveryKeys.ps1 <Command-line Arguments>`
        i. OU Example `.\Export-BitLockerRecoveryKeys.ps1 -ActiveDirectory ""OU=OurComputers,CN=Computers,DC=company,DC=local""`

4. Follow prompts to collect accounts
5. Output: CSV file *BitLockerKeys.csv*
6. Build a new image with this CSV using the **Optional - Image with Custom BitLockerKeys.csv** section above

NOTE:

- Use OU flag for large Active Directory environments where base domain searches return 1000s of computers.

Host Remediation Tools

Write ISO Files to a USB Drive

1. Download Rufus, an open-source utility for creating bootable USB sticks from https://rufus.ie/en/
2. Open Rufus:
3. Use the **Device** menu to select the desired USB drive target
   ⚠️ **WARNING: USB drive will be wiped clean**
4. Click the **Select** button (next to **Boot Selection**) and choose the *CSPERecovery* or *CSSafeBoot* ISO file
5. Use the **Partition** scheme dropdown menu to select *GPT*
6. Use the **Target System** dropdown menu to select *UEFI (non CSM)*
7. Press **Start**
8. **IMPORTANT - please carefully read the following:**
    a. If prompted to write in *ISO mode* or *ESP mode*
        i. *ISO mode* - **use this first!**
            - Most complete user experience, supports both MBR and UEFI booting, and enables the automated cleanup script *CSSafeBoot* ISO.
            - The *CSPERecovery* ISO is not impacted.
        ii. *ESP mode* - **use if host cannot recognize bootable USB drive** (particularly on older UEFI systems)
            - Go back to Step 2 and repeat these steps and select *ESP mode*.
            - The automated cleanup script will be unavailable in *CSSafeBoot* ISO, but manual remediation steps are still available and will succeed.
            - The CSPERecovery ISO is not impacted.

Booting Windows host from USB

Once you have created a bootable USB drive using https://rufus.ie/en/ (in section above)

1. Insert USB drive into the impacted host
2. Reboot the host and enter the UEFI boot Menu using the F12 key
    - You may also try the F1, F2, F10 or F11 keys (depending on the BIOS manufacturer)
3. Select the USB drive

- Prepare to select *UEFI* if given a choice between MBR and UEFI option with the same label

4. Wait while Windows PE loads
5. Use the appropriate "**Recover**..." guide below for *CSSafeBoot* or *CSPERecovery*

Recover Windows Hosts using CSPERecovery

CSPERecovery image remediates systems automatically, and includes support for BitLocker.

1. Select recovery image USB drive in BootManager
    a. **IMPORTANT**: YOU DO NOT NEED TO MODIFY UEFI FIRMWARE SETTINGS (especially boot order)
2. If BitLocker enabled
    a. ⚠️ **WARNING: BitLocker Recovery Keys should be rotated after host remediation**
        a. If prompted, manually enter your BitLocker Recovery Key to unlock the volume
        b. If *BitLockerKeys.csv* is in use, the Recovery Key for the device will be applied
3. The recovery script will automatically remove the defective Channel File 291
    a. Deletes all files starting with `C-00000291*` located in the *C:\Windows\System32\drivers\CrowdStrike* folder
    b. The device will automatically reboot
4. The Windows host should start up normally.

Recover Windows Hosts using CSSafeBoot

CSSafeBoot image modifies the default Windows boot configuration to boot into *Safe Mode with Networking*, and reboots.

1. Select recovery image USB drive in BootManager
    a. IMPORTANT: YOU DO NOT NEED TO MODIFY UEFI FIRMWARE SETTINGS (especially boot order)
    b. NOTE: Select Continue if your system reboots into the Windows Recovery environment as a part of a prior boot loop.
    c. The host will reboot into Safe Mode after the next boot.
2. Log in as user with *Local Administrator* permissions
3. Confirm the Safe Mode banner is displayed on the desktop
4. Remediation
    a. Automatic Remediation:
        i. Open Windows Explorer and select the recovery USB drive.
            1. If recovery USB drive is not displayed in Windows Explorer, skip to Manual Remediation
        ii. Locate and right-click on the file *CSRecovery.cmd*, and select **Run as Administrator**
            1. The script will:

a. Delete all files starting with `C-00000291*` located in the `C:\Windows\System32\drivers\CrowdStrike\` folder
b. Restore Windows boot configuration back to *Normal Mode*
c. Host will reboot automatically.
d. Verify Windows loads successfully

b. Manual Remediation:
   i. Open Windows Explorer and navigate to *C:\Windows\System32\drivers\CrowdStrike*
   ii. Delete all files starting with `C-00000291*` located in the `C:\Windows\System32\drivers\CrowdStrike\` folder
   iii. Right-click on the Start menu, and click either Windows PowerShell (Admin), Command Prompt (Admin), or Terminal (Admin)
   iv. At the prompt, type the following command and press Enter:
      1. `bcdedit /deletevalue {default} safeboot`
   v. Reboot the device
   vi. Verify Windows loads successfully

Recovering Windows Hosts using PXE

The host remediation ISO files can be deployed and booted through existing PXE booting capability deployed at your business.

Due to significant differences in network and software configurations with PXE booting, we cannot recommend specific generic PXE booting instructions.

Best Practices

Using BitLocker Recovery Keys

⚠️ WARNING: BitLocker Recovery Keys should be rotated after host remediation

Safe Handling

Bootable images with BitLocker Recovery Keys

- should only be accessible to those who absolutely need them
- should be stored on password protected storage devices with disk encryption
- should be transferred over encrypted communication channels

Secure Destruction

Bootable images with BitLocker Recovery Keys

- Digital ISO Image files must be destroyed using software designed for secure deletion to ensure data cannot be recovered

- Physical storage media containing ISO images should be destroyed using methods such as shredding, incineration or crushing

Troubleshooting

Host Reboots to USB Drive Only After Remediation

If host continues to boot to recovery USB drive *after remediation*

- Solution: reconfirm the boot order in the UEFI firmware settings are correct, and pull the USB drive *after remediation*
- *NOTE: CrowdStrike remediation script does not change the UEFI boot order to avoid unnecessary BitLocker steps.*
- **IMPORTANT**: *YOU DO NOT NEED TO MODIFY UEFI FIRMWARE SETTINGS* (especially boot order)
    - Doing so may cause additional BitLocker recovery steps.

Frozen CrowdStrike Safe Mode Boot Utility

If *CSPERecovery* or *CSSafeBoot* script is unresponsive after starting Windows PE.

- Solution: Hit Enter

Recovery Image Size and Device Drivers

If the `-SkipThirdPartyDriverDownloads` flag was used to build the recovery image, and drivers that were not chosen are included.

- Solution: move (or remove) any device drivers from the *\Drivers* folder you do not want in your image
- **NOTE**: CrowdStrike only provides open source drivers for libvirt-based virtual machines (e.g., OpenStack and KVM).
    - All vendor device drivers are downloaded directly from vendor websites, using HTTPS, and cryptographically verified, at build time.

Dual and Multi Boot Windows OS and BitLocker

If CSV is not in use, the *CSPERecovery* script will only automatically remediate one Windows OS installation on hosts with dual/multi-boot configurations

- Solution: repeat steps from **Recover Windows Hosts using CSPERecovery** section (above) for each Windows OS installation drive letter you want to remediate.
    - **NOTE**: each Windows OS installation device drive requires a BitLocker recovery key.

- The tool will only automatically remediate all unencrypted drives, or BitLocker protected devices if the *BitLockerKeys.csv* is used.
    - NOTE: if host is dual/multi OS boot, with BitLocker, and recovery image has CSV, all drives having keys in *BitLockerKeys.csv* will be remediated.

BitLocker Recovery Key export from Active Directory/Entra ID

- Existing CSV
    - If *.\Export-BitLockerRecoveryKeys.ps1* fails with a CSV file exists error.
        - Solution: move existing file outside your work directory (e.g. *C:\falcon-windows-host-recovery-main*).
        - The script will not automatically overwrite this file.
- Active Directory Export:
    - If *.\Export-BitLockerRecoveryKeys.ps1* fails due to permissions.
        - Solution: user must have Domain Administrator permissions, or be a member of a group delegated with read access to BitLocker Recovery Keys.
    - If AD stored keys do not appear when script run from host not connected to domain.
        - Solution: run *.\Export-BitLockerRecoveryKeys.ps1* script from a domain-joined server host.
        - Entra ID stored keys can also be exported if the AD-joined server has the required outbound network connectivity.
- Entra ID Export:
    - If *.\Export-BitLockerRecoveryKeys.ps1* fails due to permission errors.
        - Solution: the user running the script must have Administrator permissions for the required scopes.
        - Solution: the user running the script must have the **BitLockerKey.ReadBasic.All** and **Device.Read.All** scopes assigned.
            - NOTE: Global Administrator approval is required for scope assignment.
    - If *.\Export-BitLockerRecoveryKeys.ps1* fails due to a network error.
        - Solution: run *.\Export-BitLockerRecoveryKeys.ps1* from a host with connectivity to the Microsoft Graph API.

BitLocker Recovery Key CSV

Verify your CSV file has column headers that exactly match **KeyID** and **RecoveryKey.**

Additional Information

authority to bind such Entity and such Entity agrees to be bound by this Agreement. CrowdStrike grants Entity a non-exclusive, non-transferable, non-sublicensable, royalty free and limited license to access and use the Tools solely for Entity's internal business purposes, including without limitation the rights to copy and modify the Tools as necessary for your internal purposes. Any third-party software, files, drivers or other components accessed and/or downloaded by You when using a Tool may be governed by additional terms or by a separate license provided or maintained by the third party provider. THE TOOLS ARE PROVIDED "AS-IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY OR OTHERWISE. CROWDSTRIKE SPECIFICALLY DISCLAIMS ALL SUPPORT OBLIGATIONS AND ALL WARRANTIES, INCLUDING WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. IN NO EVENT SHALL CROWDSTRIKE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE TOOLS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THIS TOOL IS NOT ENDORSED BY ANY THIRD PARTY.