CROWDSTRIKE

BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager

Published Date: July 19, 2024

Objective

» BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager

Applies To

» Supported versions of the Falcons sensor for Windows

» Supported versions of Microsoft Windows

» Ivanti Endpoint Manager

» May be related to Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19 (/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19)

Procedure

1. **Retrieve BitLocker Recovery Keys –** Use Ivanti Endpoint Manager to retrieve BitLocker recovery keys:

   a. Open the Ivanti Endpoint Manager console

   b. Navigate to Security and Compliance > BitLocker

   c. Select the specific device and view the recovery key

2. **Develop a PowerShell Script –** The script will handle booting into safe mode, changing the registry key, and rebooting into normal mode. However, since BitLocker is enabled, you'll need to ensure you have the recovery key.

```
# CrowdStrikeFix.ps1
# This script deletes the problematic CrowdStrike driver file causing BSODs and reverts
Safe Mode

$filePath = "C:\Windows\System32\drivers\C-00000291*.sys"
$files = Get-ChildItem -Path $filePath -ErrorAction SilentlyContinue

foreach ($file in $files) {
   try {
            Remove-Item -Path $file.FullName -Force
            Write-Output "Deleted: $($file.FullName)"
   } catch {
            Write-Output "Failed to delete: $($file.FullName)"
   }
}

# Revert Safe Mode Boot after Fix
bcdedit /deletevalue {current} safeboot
Restart-Computer -Force
```

3. Retrieve BitLocker Recovery Keys:

a. Use Azure AD to retrieve BitLocker recovery keys

b. Navigate to Azure AD > Devices > All Devices

c. Click on the specific device and select “Show Recovery Key"

d.
```
# Example of retrieving BitLocker recovery key
$bitLockerKey = Get-BitLockerVolume | Select-Object -ExpandProperty KeyProtector | Where-Object {
$_.KeyProtectorType -eq 'RecoveryPassword' } | Select-Object -ExpandProperty RecoveryPassword
```

4. Deploy the Script Using Ivanti Endpoint Manager

a. Create a Software Distribution Package:

i. In the Ivanti Endpoint Manager console, go to Software Distribution > Packages

ii. Create a new package and add the PowerShell script

b. Distribute the Package:

i. Right-click the package and select Distribute

ii. Choose the target devices and distribute the package

c. Deploy the Package – Schedule the deployment to run on the target devices

5. Monitor and Validate

a. Monitor the deployment process through the Ivanti console

b. Validate that the machines boot correctly into normal mode after the script runs

Additional Information

» **Ivanti Compliance Settings:** Use Ivanti Compliance Settings to monitor and ensure BitLocker compliance

» **Windows Admin Center:** Use Windows Admin Center for easier management and monitoring of your devices

» **Backup:** Ensure you have backups of important data before making changes to registry and system files

» **CrowdStrike Support Portal Link:** https://supportportal.crowdstrike.com/s/article/ka16T000001tImtQAA