Microsoft guidance for applying Secure Boot DBX update (KB4575994)

[See the products that this article applies to.](https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-boot-dbx-update-kb4575994-e3b9e4cb-a330-b3ba-a602-15083965d9ca#bkmk_applies_to)

Summary

On July 29, 2020, Microsoft published [security advisory 200011](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011) that describes a new vulnerability that’s related to Secure Boot. Devices that trust the Microsoft third-party Unified Extensible Firmware Interface (UEFI) Certificate Authority (CA) in their Secure Boot configuration may be susceptible to an attacker who has administrative privileges or physical access to the device.

This article provides guidance to apply the latest Secure Boot DBX revocation list to invalidate the vulnerable modules. Microsoft will push an update to Windows Update to address this vulnerability in Spring of 2022.

The Secure Boot update binaries are hosted on [this UEFI webpage](https://uefi.org/revocationlistfile).  
  
The posted files are as follows:

* UEFI Revocation List File for x86 (32 bit)
* UEFI Revocation List File for x64 (64 bit)
* UEFI Revocation List File for arm64

After these hashes are added to the Secure Boot DBX on your device, those applications will no longer be allowed to load.

**Important:**This site hosts files for every architecture. Each hosted file includes only the hashes of applications that apply to the specific architecture. You must apply one of these files to every device, but make sure that you apply the file that is relevant to its architecture. Although it is technically possible to apply an update for a different architecture, not installing the appropriate update will leave the device unprotected.

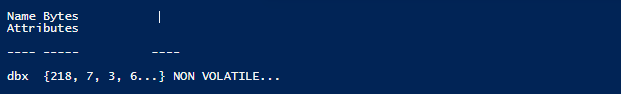
**Caution:** Read the main advisory article about this vulnerability before you try any of these steps. Incorrectly applying DBX updates could prevent your device from starting.  
  
You should follow these steps only if the following conditions are true:

* You have verified that your device trusts the third-party UEFI CA in your Secure Boot configuration. To do this, run the following line of PowerShell from an administrative PowerShell session:  
    
  [System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Microsoft Corporation UEFI CA 2011'
* You do not rely on starting any of the boot applications that are being blocked by this update.

More information

Applying a DBX update on Windows

After you read the warnings and verify that your device is compatible, follow these steps to update the Secure Boot DBX:

1. Download the appropriate UEFI Revocation List File (Dbxupdate.bin) for your platform from [this UEFI webpage](https://uefi.org/revocationlistfile).
2. You have to split the Dbxupdate.bin file into the necessary components in order to apply them by using PowerShell cmdlets. To do this, follow these steps:
   1. Download the PowerShell script from [this PowerShell Gallery webpage](https://aka.ms/DbxSplitScript).
   2. Run the following PowerShell script on the Dbxupdate.bin file:  
        
      **SplitDbxContent.ps1 “c:\path\to\file\dbxupdate.bin**
   3. Verify that the command created the following files:  
        
      "Applying" step 2c command output
      * Content.bin – update contents
      * Signature.p7 – signature authorizing the update process
3. In an administrative PowerShell session, run the **Set-SecureBootUefi** cmdlet to apply the DBX update:  
     
   **Set-SecureBootUefi -Name dbx -ContentFilePath .\content.bin -SignedFilePath .\signature.p7 -Time 2010-03-06T19:17:21Z -AppendWrite  
     
   Expected output**  
     
   
4. Restart the device to complete the update installation process.

For more information about the Secure Boot configuration cmdlet and how to use it for DBX updates, see [Set-Secure.](https://docs.microsoft.com/en-us/powershell/module/secureboot/set-securebootuefi)

Verifying that the update was successful

After you successfully complete the steps in the previous section and restart the device, follow these steps to verify that the update was applied successfully. After successful verification, your device will no longer be affected by the GRUB vulnerability.

1. Download the DBX update verification scripts from [this GitHub Gist webpage](https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0).
2. Extract the scripts and binaries from the compressed file.
3. Run the following PowerShell script within the folder that contains the expanded scripts and binaries to verify the DBX update:   
     
   **Check-Dbx.ps1 .\dbx-2021-April.bin'**

**Note:** If a DBX update that matches the July 2020 or October 2020 versions from [this revocation list file archive](https://uefi.org/revocationlistfile) was applied, run the following appropriate command instead:   
  
**Check-Dbx.ps1 '.\dbx-2020-July.bin'**

**Check-Dbx.ps1 '.\dbx-2020-October.bin'**

1. Verify that the output matches the expected result:  
     
   "Verifying" step 4 command output

FAQ

**Q1: What does the error message "Get-SecureBootUEFI: Cmdlets not supported on this platform" mean?**

**A1:** This error message indicates that NO Secure Boot feature is enabled on the computer. Therefore, this device is NOT affected by the GRUB vulnerability. No further action is necessary.

**Q2: How do I configure the device to trust or not trust third-party UEFI CA?**

**A2:** We recommend that you consult your OEM vendor.

For Microsoft Surface, change the Secure Boot setting to “Microsoft Only,” and then run the following PowerShell command (the result should be “False”):

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Microsoft Corporation UEFI CA 2011'

For more information about how to configure for Microsoft Surface, see [Manage Surface UEFI settings - Surface | Microsoft Docs](https://docs.microsoft.com/en-us/surface/manage-surface-uefi-settings).

**Q3: Does this problem affect Azure IaaS Generation 1 and Generation 2 virtual machines?**

**A3:** No. Azure guest virtual machines Gen1 and Gen2 do not support the Secure Boot feature. Therefore, they are unaffected by the chain of trust attack.

**Q4: Do ADV200011 and CVE-2020-0689 refer to the same vulnerability that's related to Secure Boot?**

**A:** No. These security advisories describe different vulnerabilities. "ADV200011" refers to a vulnerability in GRUB (Linux component) that could cause a Secure Boot bypass. "CVE-2020-0689" refers to a security feature bypass vulnerability that exists in Secure Boot.

**Q5: I can't run either of the PowerShell scripts. What should I do?**

**A:** Verify the PowerShell execution policy by running the **Get-ExecutionPolicy** command. Depending on the output, you might have to update the execution policy:

* [Set-ExecutionPolicy (Microsoft.PowerShell.Security) - PowerShell | Microsoft Docs](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.1)

Third-party information disclaimer

Third-party contact disclaimer

**Applies to:**

Windows 10 for 32-bit Systems  
Windows 10 for x64-based Systems  
Windows 10 Version 2004 for 32-bit Systems  
Windows 10 Version 2004 for ARM64-based Systems  
Windows 10 Version 2004 for x64-based Systems  
Windows 10 Version 1909 for 32-bit Systems  
Windows 10 Version 1909 for ARM64-based Systems  
Windows 10 Version 1909 for x64-based Systems  
Windows 10 Version 1903 for 32-bit Systems  
Windows 10 Version 1903 for ARM64-based Systems  
Windows 10 Version 1903 for x64-based Systems  
Windows 10 Version 1809 for 32-bit Systems  
Windows 10 Version 1809 for ARM64-based Systems  
Windows 10 Version 1809 for x64-based Systems  
Windows 10 Version 1803 for 32-bit Systems  
Windows 10 Version 1803 for ARM64-based Systems  
Windows 10 Version 1803 for x64-based Systems  
Windows 10 Version 1709 for 32-bit Systems  
Windows 10 Version 1709 for ARM64-based Systems  
Windows 10 Version 1709 for x64-based Systems  
Windows 10 Version 1607 for 32-bit Systems  
Windows 10 Version 1607 for x64-based Systems  
Windows 8.1 for 32-bit systems  
Windows 8.1 for x64-based systems  
Windows RT 8.1  
Windows Server, version 2004 (Server Core installation)  
Windows Server, version 1909 (Server Core installation)  
Windows Server, version 1903 (Server Core installation)  
Windows Server 2019  
Windows Server 2019 (Server Core installation)  
Windows Server 2016  
Windows Server 2016 (Server Core installation)  
Windows Server 2012 R2  
Windows Server 2012 R2 (Server Core installation)  
Windows Server 2012  
Windows Server 2012 (Server Core installation)