The following explanatory information was provided to the UEFI Forum Security Response Team by the Microsoft UEFI CA with the May 9th, 2023, release of Secure Boot Revocation List. This release of dbx files specifically relates to the "Black Lotus" security vulnerability.

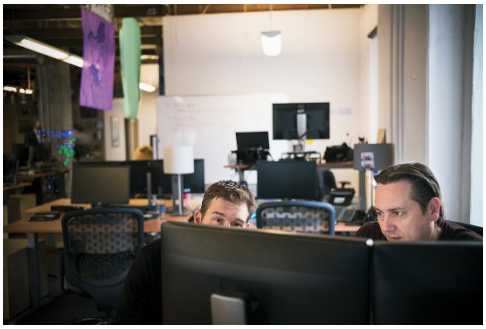
SKU SiPolicy and Black Lotus Windows Defender Application Control (WDAC) is Windows' built-in application control solution on which IT admins and Windows users can build allowlist and denylist policies. Besides the name, there is no overlap with Microsoft Defender. WDAC has a reserved platform policy type only available to Microsoft platform teams called: SKU SiPolicy. Windows enforces that the SKU SiPolicy must be signed by one of the trusted Windows' signing certificate authorities.

Beginning with Windows 10, version 1507, the Windows Boot Manager added support for parsing the SKU SiPolicy and revoking boot media. Due to the space constraints in the DBX, Windows Security teams leveraged the SKU SiPolicy to revoke the vulnerable versions of the Windows Boot Manager. Boot Manager versions beginning with Windows 10, version 1703, added the ability to parse its own version resource. Windows 8, 8.1 and Windows 10 (prior to May 2015) Boot Manager versions do not support revocation using the SKU SiPolicy and were therefore revoked using the Secure Boot DBX blocklist.

The following is a summary of Microsoft's revocation techniques used for the Black Lotus vulnerability:

- Boot Managers from Windows 8 to Windows 10, version 1507: revoked by DBX entries
- Boot Managers from Windows 10, version 1507 to Windows 10, version 1607: revoked by hash by SKU SiPolicy
- Boot Managers from Windows 10, version 1703 to today: revoked by version number by SKU SiPolicy

For more information on Black Lotus and how organizations can assess whether they have been targeted and protect
themselves, please visit https://www.microsoft.com/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/



Guidance for investigating attacks using CVE-2022-21894: The BlackLotus campaign - Microsoft Security Blog

This guide provides steps that organizations can take to assess whether users have been targeted or compromised by threat actors exploiting CVE-2022-21894 via a Unified Extensible Firmware Interface (UEFI) bootkit called BlackLotus.

www.microsoft.com