BlackLotus Mitigation Guide

Executive summary

BlackLotus is a recently publicized malware product garnering significant attention within tech media. Similar to 2020's BootHole (CVE-2020-10713), BlackLotus takes advantage of a boot loader flaw—specifically CVE-2022-21894 Secure Boot bypass known as "Baton Drop"—to take control of an endpoint from the earliest phase of software boot. Microsoft® issued patches for supported versions of Windows to correct boot loader logic. However, patches were not issued to revoke trust in unpatched boot loaders via the Secure Boot Deny List Database (DBX). Administrators should not consider the threat fully remediated as boot loaders vulnerable to Baton Drop are still trusted by Secure Boot.

As described in this Cybersecurity Information Sheet (CSI), NSA recommends infrastructure owners take action by hardening user executable policies and monitoring the integrity of the boot partition. An optional advanced mitigation is to customize Secure Boot policy by adding DBX records to Windows® endpoints or removing the Windows Production CA certificate from Linux® endpoints.

BlackLotus boot security threat

NSA recognizes significant confusion regarding the threat posed by BlackLotus. Some organizations use terms like "unstoppable," "unkillable," and "unpatchable" to describe the threat. Other organizations believe there is no threat due to patches that Microsoft released in January 2022 and early 2023 for supported versions of Windows. [1] The risk exists somewhere between both extremes.

BlackLotus shares some characteristics with Boot Hole (CVE-2020-10713). [2] Instead of breaking the Linux boot security chain, BlackLotus targets Windows boot by exploiting a flaw in older boot loaders—also called boot managers—to set off a chain of malicious actions that compromise endpoint security. Exploitation of Baton Drop (CVE-2022-21894) allows BlackLotus to strip the Secure Boot policy and prevent its enforcement. Unlike Boot Hole, the vulnerable boot loaders have not been added to the Secure Boot DBX revocation list. Because the vulnerable boot loaders are not listed within the DBX, attackers can substitute fully patched boot loaders with vulnerable versions to execute BlackLotus.

NSA recommends system administrators within DoD and other networks take action. BlackLotus is not a firmware threat, but instead targets the earliest software stage of boot.

Defensive software solutions can be configured to detect and prevent the installation of the BlackLotus payload or the reboot event that starts its execution and implantation. NSA believes that currently published patches could provide a false sense of security for some infrastructures. Because BlackLotus integrates Shim and GRUB into its implantation routine, Linux administrators should also be vigilant for variants affecting popular Linux distributions.

Mitigation recommendations

Action 1: Update recovery media and activate optional mitigations

Recommended for all Windows infrastructures. Not applicable to Linux infrastructures. NSA recommends Windows administrators install the latest security patches for their endpoints. Microsoft patches from May 2023 contain optional software mitigations to prevent rollback of the boot manager and kernel to versions vulnerable to Baton Drop and BlackLotus. The optional mitigations – including a Code Integrity Boot Policy – should be enabled after the organization has updated its Windows installation, recovery, and diagnostic software to the latest available versions. [3]

Infrastructure administrators should note that Windows 10 and 11 have applicable security updates and ongoing mitigation deployments for BlackLotus. Older, unsupported Windows versions will not receive the full complement of BlackLotus mitigation measures. Windows infrastructures should migrate to supported versions of Windows if running an unsupported release. [3]

Action 2: Harden defensive policies

Recommended for all infrastructures. The malware install process for BlackLotus places an older Windows boot loader Extensible Firmware Interface (EFI) binary into the boot partition, disables Memory Integrity, disables BitLocker, and reboots the device. Many endpoint security products (e.g., Endpoint Detection and Response, host-based security suites, user-monitoring packages) can be configured to block one or more of these events outside of a legitimate, scheduled update. Configure defensive software to scrutinize changes to the EFI boot partition in particular. Alternatively, leverage application allow lists to permit only known and trusted executables.

Action 3: Monitor device integrity measurements and boot configuration

Recommended for most infrastructures. Many endpoint security products and firmware monitoring tools provide integrity-scanning features. Configure these products and tools to monitor the composition of the EFI boot partition. Leverage these tools to look for unexpected changes in bootmgfw.efi, bootmgr.efi, or the introduction of additional unexpected EFI binaries (e.g., shimx64.efi or grubx64.efi). Changes to the boot partition are infrequent and warrant additional scrutiny.

If unexpected changes are detected within the EFI boot partition, prevent the device from rebooting. Endpoint and host defensive suites may allow creating rules or triggers that can be paired with group policies to temporarily restrict reboot. Remediate the boot partition to a known good state before permitting reboot. A reboot will execute EFI binaries and can implant BlackLotus.

Microsoft has published specific information regarding the staging of BlackLotus components, alterations to Windows registry values, and network indicators. Full specifics can be found at the Microsoft Incident Response blog. [4]

Action 4: Customize UEFI Secure Boot

4.A. Instructions for Windows infrastructures. Expertly administered and exposed infrastructures only. Not recommended due to limited long-term effectiveness.

BlackLotus relies upon older (pre-January 2022), signed Windows boot loader images to implant a system. Secure Boot can be updated with DBX deny list hashes that prevent executing older and vulnerable boot loaders. Public reporting [5] provides indications as to which boot managers are observed exploited in the wild. In 2020, NSA published "UEFI Secure Boot Customization" to provide guidance on modifying Secure Boot. Adding DBX hashes qualifies as a partial customization action covered in section 4 "Customization," starting on page 7, and continuing through section 4.4.3 “Update the DB or DBX.” [6] Additionally, a GitHub.com repository has been set up with some helpful scripts and guides to accomplish customization. [7]

Note: Adding boot loader hashes to the DBX may render many Windows install and recovery images, discs, and removable media drives unbootable. Microsoft provides updated install and recovery images for Windows 11 and 10. Only update the DBX after acquiring install and recovery media with the January 2022 or later patch assortment applied (e.g., version 22H1 or newer).

Warning: The following DBX hashes may be combined with the Secure Boot Customization steps to revoke trust in select boot loaders vulnerable to Baton Drop. [6] However, more vulnerable boot loaders exist than the DBX can contain. BlackLotus developers can rapidly switch to alternate vulnerable boot loaders to evade DBX customization. Mitigating BlackLotus via DBX updates is not recommended. Action 1’s patches and optional mitigations are recommended instead.

Table: DBX hashes

#	UEFI Secure Boot DBX Hashes
1	B22A7B3CEBB32C80C36EAABB6F77D164AE8B76BF161F423B6E2FBF9DCBC96C02
2	D355041DFBA41F8AE2CE6766ECBC88C93A743FC74F95E7E7AA3EF32CA6E4B390
3	D9F629F6D1D83AC7A15DCB1116E4B9BF128758EC2EA389AA1E0DA3B8F2951150
4	53FCE58746C4B042B101B8682B4E52CE8B620D3C68F69034996E33D3DDDCA1FF
5	F7357DD5000E1FBADBF17CC6025243A243D1BFA705801051119277A30D717B71
6	39C6475B3F00D92EEC049D8F6EFA010CB06F1240ED1CE7E40611278C73817471
7	2E094D21DC457CC4826FCD48395B92DC782F978EEF8210E4B6F5E708527907FF
8	BFE0E68889A750E699788C11F08AFAE940770ED83C1B4A5DB27E10933B29CAD1

4.B. Instructions for Linux infrastructures. Expertly administered and exposed infrastructures only.

Linux system administrators may forego adding DBX hashes in favor of removing the Microsoft Windows Production CA 2011 certificate from Secure Boot’s DB. The total number of Baton Drop-vulnerable boot loaders signed by the key associated with the Production CA’s certificate is thought to exceed the available DBX memory. Removing the certificate negates the need to add DBX entries related to Baton Drop and BlackLotus. Linux administrators will still need the Microsoft Unified Extensible Firmware Interface (UEFI) Third Party Marketplace CA 2011 certificate to utilize Secure Boot with leading Linux distributions. [6]

Do not place the Windows Production CA 2011 certificate in the Machine Owner Key Exclusion (MOKX) list in lieu of removing it from the DB. Utilizing MOKX in this way will cause the revoked certificate to still be trusted between firmware initialization and the initialization of Shim’s Secure Boot extensions.

The Windows Production CA 2011 certificate must be restored if converting the device from Linux to Windows. Microsoft provides the certificate for download via their resources for system manufacturers. [9]

Frequently asked questions

1. Is BlackLotus a firmware implant?

No. BlackLotus is boot software. The UEFI boot process involves several phases. Execution control flow transitions from firmware to software following the Boot Device Select phase. [8]

2. Can BlackLotus be removed or quarantined?

Yes, prior to execution. Devices that boot to a BlackLotus EFI binary will need to be completely reimaged. Attempts to remove BlackLotus following installation result in kernel errors.

3. Does BlackLotus bypass Secure Boot?

An initial bypass is followed by poisoning that configures Secure Boot to trust the malware. An older, vulnerable boot loader that is trusted by Secure Boot is necessary to strip the Secure Boot policy from being enforced so that BlackLotus can implant its entire software stack. Subsequent boots extend the Microsoft UEFI signing ecosystem with a malicious BlackLotus certificate. Thus, Secure Boot will trust the malware.

4. Which version of Windows is affected?

BlackLotus targets Windows 11 and 10. Variants may exist to target older, UEFI-booting versions of Windows. Patches are available for Windows 8.1, 10, and 11.

5. Is Linux affected? Is there a version of BlackLotus that targets Linux?

No, not that has been identified at this time. BlackLotus does incorporate some Linux boot binaries, but the malware targets Windows OS software. No Linux-targeting variant has been observed.

6. Is BlackLotus really unstoppable?

No – BlackLotus is very stoppable on fully updated Windows endpoints, Secure Boot-customized devices, or Linux endpoints. Microsoft has released patches and continues to harden mitigations against BlackLotus and Baton Drop. [1], [3], [4] The Linux community may remove the Microsoft Windows Production CA 2011 certificate on devices that exclusively boot Linux. Mitigation options available today will be reinforced by changes to vendor Secure Boot certificates in the future (some certificates are expiring starting in 2026).

7. Where can I find more public information?

NSA is aware of several technically deep analysis reports posted online from security researchers and vendors. One thorough source of public information is ESET Security's blog referenced as [5] in this report. Another source of information is the Microsoft Security Response Center. [3], [4]

8. Should I reconfigure Secure Boot?

No. Secure Boot is best left enabled in standard mode. Only advanced infrastructures and expert administrators should engage the custom/user-defined mode. Some security software may require additional certificates or hashes to be added to the DB allow list or DBX deny list. No one should disable Secure Boot on an endpoint built within the past 5 years.

9. Can a Trusted Platform Module (TPM) stop BlackLotus?

No. A TPM can only detect BlackLotus. Implant boot binaries are delivered to the EFI boot partition after the TPM has recorded boot time measurements. Upon the next reboot, the TPM captures measurements showing a BlackLotus infection. However, a TPM can only detect – not prevent – implantation as the TPM is an observer and container of integrity indicator data. A TPM does not have an active enforcement capability.

In a Network Access Control (NAC) infrastructure based on TPM attestation, NAC would prevent infected machines from accessing protected resources by indicating changes in Platform Configuration Registers (PCRs) 4-7. NAC also provides an opportunity to remediate affected endpoints prior to connecting to a protected resource.

10. Can TPM-extended Shim / TrustedShim (T-Shim) stop BlackLotus?

No. T-Shim checks TPM measurements recorded prior to the main boot loader. Secure Boot is responsible for enforcement following T-Shim.

11. What is Secure Boot customization?

Customization involves one of the following:

- **Partial customization** – augmenting the Microsoft and system vendor Secure Boot ecosystem with additional DB and DBX entries as necessary to enable signature and hash checks on unsupported/custom software or block unwanted software.
- **Full customization** – replacing all vendor and Microsoft certificates and hashes with those generated and selected by the infrastructure owner (requires specialized knowledge of hardware values).

12. How does BlackLotus compare to Boot Hole?

Boot Hole involved flaws in Secure Boot-signed GRUB boot loaders. A configuration file could be created to cause buffer overflows and arbitrary code execution at boot time. Secure Boot could be ignored and completely bypassed.

BlackLotus is sophisticated malware observed in the wild. It exploits a flaw (known as Baton Drop) in Secure Boot-signed copies of the Windows Boot Manager to truncate the Secure Boot policy values. Instead of stopping due to the lack DB and DBX values, the vulnerable boot manager allows boot to continue. BlackLotus injects a version of Shim utilizing its own Machine Owner Key (MOK) – similar to the allow list DB – to vouch for signatures on its own malicious binaries. The result is Secure Boot remains enforcing while silently poisoned and permitting malware to execute.

13. Why doesn't NSA recommend setting up a custom Secure Boot ecosystem as a mitigation?

NSA has internally piloted efforts to exclusively rely on custom certificates and hashes to define Secure Boot policy. Pilot efforts have proven effective at preventing threats like BlackLotus, Baton Drop, BootHole, and similar prior to discovery. However, the administrative overhead and vendor collaboration necessary represent a resource investment not appropriate for most enterprise infrastructures. The process of fully customizing Secure Boot is also not capable of being automated outside of a narrow selection of workstation and server products.

14. Can Trusted eXecution Technology (TXT) stop BlackLotus?

Yes, if and only if the TPM non-volatile memory (NVRAM) policy is set to boot a specific boot loader. In practice, setting a specific boot loader has caused administrative challenges when handling updates that affect the EFI boot partition. TXT is not a recommended mitigation given the likelihood to render endpoints temporarily unbootable.

15. Are virtual machines affected?

Yes. VMs boot into a virtual UEFI environment. BlackLotus targets the OS software boot loaders that execute following the virtual firmware initialization.

Works cited

[1] Microsoft Security Response Center (2022), January 2022 Security Updates. https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

[2] Eclypsium (2020), There's a Hole in the Boot. https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot

[3] Microsoft Security Response Center (2023), KB5025885: How to manage the Windows Boot Manager revocations for Secure Boot changes associated with CVE-2023-24932. https://support.microsoft.com/help/5025885

[4] Microsoft Incident Response (2023), Guidance for investigating attacks using CVE-2022-21894: The BlackLotus campaign. https://www.microsoft.com/en-us/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign

[5] Smolar, Martin (2023), BlackLotus UEFI Bootkit: Myth Confirmed. https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed

[6] National Security Agency (2020), UEFI Secure Boot Customization [S/N: U/OO/168873-20]. https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF

[7] National Security Agency (2020), UEFI Secure Boot Customization. https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance/tree/master/secureboot

[8] Carnegie Mellon University (2022), UEFI – Terra Firma for Attackers. https://insights.sei.cmu.edu/blog/uefi-terra-firma-for-attackers/

[9] Microsoft (2022), Windows Secure Boot Key Creation and Management Guidance. https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. This guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Questions and Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov