PROTECTLI
TAKE BACK YOUR NETWORK

Technical Service Bulletin TSB-2026-003

Expiring Microsoft Secure Boot Certificates

Issue Date	June 24, 2026
Last Updated	June 24, 2026
Version	1.0.0
Severity	HIGH
Affected Products	Systems using Secure Boot signed by Microsoft. See Affected Systems section below
Affected Firmware	AMI BIOS (all versions, except V Series)
Affected Components	Secure Boot: Key Exchange Key (KEK) and Signature Database (db) certificates
Status	WORKAROUND AVAILABLE | FIX IN DEVELOPMENT

Changelog

Version	Date	Changes
1.0.0	June 24, 2026	Initial release

Executive Summary

> **Scope:** This bulletin applies only to systems that are actively using Secure Boot. If Secure Boot is disabled on your unit, this issue does not affect you and no action is required.

Several Microsoft certificates used by the Secure Boot feature are approaching their expiration dates in 2026. These certificates are enrolled in the Secure Boot Signature Database (db) and Key Exchange Key (KEK) on affected Protectli units. Once a certificate expires, it can no longer be used to sign updates to the Secure Boot databases, which means the affected units will not be able to receive new Secure Boot key updates, revocation list updates, or related early-boot security protections until the firmware is updated with the 2023-

series certificates.

In most cases, an expired certificate does not prevent an operating system that is already installed from booting. Microsoft has stated that Windows will continue to boot on devices that have not received the 2023 certificates. Linux distributions that support Secure Boot are also expected to continue booting on the existing 2011 certificates.

> **Important:** The first affected certificate, the Microsoft Corporation KEK CA 2011, expires on **June 24, 2026**. After this date, affected units can no longer receive signed updates to the db or dbx using that key. If you have Secure Boot enabled, review this bulletin to determine whether your configuration is affected.

A permanent firmware fix that enrolls the updated 2023-series Microsoft certificates is currently in development. If a unit is affected to the point that the operating system will not boot, the recommended workaround is to disable Secure Boot. If a unit is not affected, the recommendation is to leave Secure Boot enabled until the firmware update with the new certificates is available. Additional workarounds that preserve Secure Boot functionality during the transition are under investigation and will be documented in future revisions of this bulletin.

Affected Systems

Overview

This issue affects AMI BIOS units where Secure Boot is enabled and the firmware's enrolled certificates include only the expiring 2011-series Microsoft certificates, without the replacement 2023-series certificates. coreboot-based units are not affected, as the correct 2023-series certificates are already enrolled.

AMI BIOS Units

All Protectli units running AMI BIOS firmware with Secure Boot enabled are potentially affected, with the following exception:

- **V Series (V1210, V1211, V1410, V1610):** These units already have the correct 2023-series Microsoft certificates enrolled and are not affected.

coreboot Units

Protectli coreboot-based units are not affected by this issue. The correct 2023-series Microsoft certificates are already enrolled on these units. For reference, the following models do not support Secure Boot at all:

- **FW Series:** Legacy (non-UEFI) firmware only. Secure Boot is not supported and therefore not applicable.
- **FW4C:** UEFI firmware, but Secure Boot is not available (disabled at the platform level).

> **Note:** This issue only applies to units where Secure Boot is currently **enabled**. Units with Secure Boot disabled are not affected and do not require immediate action, though a firmware update will still be provided to ensure future compatibility.

Operating Systems

The following operating systems may be affected if they rely on the expiring certificates for Secure Boot authentication:

- Windows (all versions using Microsoft Windows Production PCA 2011 or Microsoft UEFI CA 2011)
- Linux distributions that support Secure Boot (Ubuntu, Debian, Fedora, and others that rely on a signed shim verified by Microsoft UEFI CA 2011)

Problem Description

What Is Secure Boot?

Secure Boot is a UEFI firmware security feature that verifies the authenticity of operating system bootloaders and drivers before allowing them to run. It uses a hierarchy of cryptographic keys and certificates stored in the firmware to perform this verification:

- **Platform Key (PK):** The root of trust. Authorizes updates to the Key Exchange Key (KEK). Protectli's PK was provisioned by Protectli during manufacturing.
- **Key Exchange Key (KEK):** Authorizes updates to the Signature Database (db) and Forbidden Signature Database (dbx).
- **Signature Database (db):** Contains the certificates used to verify bootloaders, OS kernels, and option ROMs. A bootloader must be signed by a certificate present in the db to be allowed to run.
- **Forbidden Signature Database (dbx):** Contains revoked certificates and hashes. Any binary matching an entry in the dbx will be blocked, even if it would otherwise pass db verification.

Which Certificates Are Expiring?

The following Microsoft certificates, currently enrolled in affected units, are expiring in 2026:

Certificate	Store	Expiration Date	Purpose	Replacement
Microsoft Corporation KEK CA 2011	KEK	**June 24, 2026**	Authorizes updates to the db and dbx	Microsoft Corporation KEK 2K CA 2023
Microsoft Corporation UEFI CA 2011	db	**June 27, 2026**	Authenticates third-party bootloaders and EFI applications (including Linux shim)	Microsoft UEFI CA 2023
Microsoft Windows Production PCA 2011	db	**October 19, 2026**	Authenticates the Windows OS bootloader	Windows UEFI CA 2023

> **Note:** The 2023-series replacement certificates (Microsoft Corporation KEK 2K CA 2023, Microsoft UEFI CA 2023, Windows UEFI CA 2023, and Microsoft Option ROM UEFI CA 2023) are the current standard and are not affected by this issue. The firmware update in development will enroll these certificates.

Symptoms and Effects

The effects of certificate expiration depend on how the unit is configured and which operating system is in use. The following may be observed once the relevant certificate expires:

- **Secure Boot key updates blocked:** This is the primary and most universal effect. Once the KEK CA 2011 certificate expires (June 24, 2026), the firmware can no longer accept signed updates to the db or dbx using that key. The unit will not receive new Secure Boot database updates, revocation list (dbx) updates, or related early-boot security protections until the firmware is updated with the 2023-series certificates.
- **Windows continues to boot:** Microsoft has stated that Windows will continue to start and operate normally on devices that have not received the 2023 certificates, and standard Windows updates will continue to install. An installed Windows OS is not expected to stop booting as a direct result of these certificates expiring.
- **Linux distributions generally continue to boot:** Linux distributions that support Secure Boot are expected to continue booting on the existing 2011 certificates. However, if a distribution updates its shim (this is distribution dependent) so that it is signed only with the 2023 certificates and no longer relies on the 2011 certificates, the OS may fail to boot if the 2023 certificates are not enrolled on the unit.
- **Other certificate-dependent functions may stop working:** If the expiring certificates are used for purposes beyond OS boot, those services may not work as expected after expiration.

If a boot failure does occur, the system may display a Secure Boot violation error or fail to load the OS.

Important Clarifications

> **Data is not at risk.** Certificate expiration does not erase, corrupt, or modify any data stored on the system. The operating system and all stored files remain intact. This issue affects only the firmware's Secure Boot verification and key-update process, not stored data.

Workaround

Determine Whether Your Unit Is Affected

Before changing any settings, determine whether your unit is actually affected. If your operating system continues to boot normally with Secure Boot enabled, no immediate action is required, and the recommendation is to leave Secure Boot enabled until the firmware update with the 2023-series certificates is available. If your operating system will not boot due to Secure Boot, the unit is affected and the workaround below applies.

If Affected: Disable Secure Boot

If the operating system will not boot, the simplest workaround is to disable Secure Boot in the firmware settings. With Secure Boot disabled, the firmware will not attempt to verify bootloaders against the certificate stores, and the operating system will boot normally.

Disabling Secure Boot does not affect data integrity or general system stability. It removes the boot-time

cryptographic verification of the OS, which is a security feature rather than a functional requirement for the system to operate.

How to Disable Secure Boot: AMI BIOS

1. Reboot the system and enter the BIOS/firmware setup utility by pressing the `Del` button
2. Navigate to the **Security** tab
3. Navigate to the **Secure Boot** option and press `Enter`
4. In the Secure Boot menu, navigate to the **Secure Boot** option
5. Press `Enter`
6. Select the **Disable** option
7. Press `Enter` again to set the option
8. Save changes and reboot by pressing `F4`
9. The system will reboot and the OS should load normally

> **Note:** The exact menu path may vary slightly depending on the specific product and BIOS version. If you are unable to locate the Secure Boot option, contact support for guidance specific to your model.

Additional Workarounds Under Investigation

Protectli is currently investigating additional workarounds that would allow users to maintain Secure Boot functionality while the firmware update is in development. These may include manual enrollment of the 2023-series certificates through the firmware's Key Management interface. This bulletin will be updated when additional guidance is available.

> **Note:** Microsoft has indicated that it will manage the certificate update process automatically on a significant portion of Windows devices. It is possible that Windows may enroll the updated Secure Boot certificates automatically on affected units. Protectli is verifying this behavior and will update this bulletin with findings.

Permanent Resolution

Protectli is developing firmware updates for all affected products that will enroll the current 2023-series Microsoft Secure Boot certificates alongside or in replacement of the expiring 2011-series certificates. This update will restore full Secure Boot functionality without requiring manual intervention.

The updated certificate set to be enrolled includes:

- **KEK:** Microsoft Corporation KEK 2K CA 2023
- **db:** Microsoft UEFI CA 2023 (replaces Microsoft UEFI CA 2011)
- **db:** Windows UEFI CA 2023 (replaces Microsoft Windows Production PCA 2011)
- **db:** Microsoft Option ROM UEFI CA 2023 (replaces Microsoft UEFI CA 2011 for option ROMs)

Customers will be notified through the following channels when firmware updates are available:

- Email notification to registered customers
- Announcement on the Protectli website

Impact on System Operation

- **Secure Boot updates:** Once the certificates expire, affected units can no longer receive signed Secure Boot database (db/dbx) updates or related early-boot security protections until the firmware is updated with the 2023-series certificates. This is the primary effect for most units.
- **Boot functionality:** In most cases the installed operating system continues to boot normally. Boot failures are limited to specific scenarios, such as a Linux distribution whose shim has been re-signed to rely only on the 2023 certificates that are not yet enrolled. Where a boot failure does occur, disabling Secure Boot resolves it.
- **Data integrity:** No data loss or corruption. All data on storage devices remains intact and accessible.
- **System stability:** No system crashes or instability are caused by this issue.
- **Security posture:** Disabling Secure Boot as a workaround removes boot-time OS verification. For environments with strict security requirements, consult your security policy regarding the acceptability of this workaround until the firmware update is available.
- **Other functionality:** All other system functions, network interfaces, and connected devices are unaffected, unless a service on the unit relies on the expiring certificates for a purpose other than OS boot.

Frequently Asked Questions

Q: How do I know if my system has Secure Boot enabled?

A: You can check in the firmware setup utility (BIOS/UEFI). On Windows, you can also open the System Information tool (`msinfo32`) and look for the "Secure Boot State" field. On Linux, the command `mokutil --sb-state` will report whether Secure Boot is currently enabled.

Q: Will this issue affect me if Secure Boot is disabled?

A: No. If Secure Boot is already disabled, the certificates are not used during the boot process and the expiration has no effect on your unit. A firmware update will still be released for your unit to ensure future readiness if you choose to enable Secure Boot later.

Q: Will my operating system stop booting when the certificates expire?

A: In most cases, no. Microsoft has stated that Windows will continue to boot and operate normally on devices that have not received the 2023 certificates. Linux distributions that support Secure Boot are also expected to continue booting on the existing 2011 certificates. The main exception is a Linux distribution that updates its shim to rely only on the 2023 certificates; in that case, the OS may fail to boot if the 2023 certificates are not enrolled on the unit. The primary effect of expiration is that the unit can no longer receive Secure Boot key and database updates until the firmware is updated.

Q: Are OPNsense or pfSense affected?

A: No. OPNsense and pfSense® are FreeBSD-based and do not support Secure Boot. These systems require Secure Boot to be disabled in order to boot, so the expiring certificates play no role and these systems are not affected by this issue.

Q: Which expiration date should I be most concerned about?

A: The Microsoft Corporation KEK CA 2011 expires first, on June 24, 2026. After that date, the unit can no longer receive signed updates to the Secure Boot databases. The Microsoft Corporation UEFI CA 2011 follows on June 27, 2026, and the Microsoft Windows Production PCA 2011 expires on October 19, 2026. These dates govern when the corresponding certificates can no longer sign new updates. They do not, by themselves, mean an installed OS will stop booting on those dates.

Q: Will disabling Secure Boot delete or affect my data?

A: No. Disabling Secure Boot has no effect on data stored on your drives. It only changes whether the firmware cryptographically verifies the OS bootloader before loading it.

Q: Will the firmware update require me to re-enroll my operating system or re-install anything?

A: No reinstallation of the operating system is expected to be required. The firmware update will update the certificate stores; your existing OS installation, signed with current Microsoft certificates, should continue to work normally. Specific guidance will be provided with the firmware update when available.

Support and Contact Information

If you have questions about this issue, you can reach out to us at:

- **Email Support:** support@protectli.com
- **Support Portal:** Open a ticket through your Protectli account
- **Additional Contact Options:** https://protectli.com/contact/

Document Information

TSB Number	TSB-2026-003
Issue Date	June 24, 2026
Last Updated	June 24, 2026
Version	1.0.0

© 2026 Protectli. All rights reserved. This document may be reproduced and distributed for customer support purposes.