

Product Security Information

Microsoft 2011 Secure Boot Certificate Expiration

IQSIGHT-SI-2026-0601

Overview

Microsoft is replacing its 2011-era Secure Boot certificates, which begin expiring in June 2026, with a new 2023 certificate set (*Microsoft Corporation KEK CA 2023, Windows UEFI CA 2023, Microsoft UEFI CA 2023, and Microsoft Option ROM UEFI CA 2023*). The 2023 certificates extend the Secure Boot chain of trust on Windows-based devices.

Affected IQSIGHT appliances will continue to start and operate normally after the 2011 certificates expire, and standard Windows updates will continue to install. However, devices that do not receive the 2023 certificates will no longer be able to apply new early-boot security updates, including updates to the Windows Boot Manager, Secure Boot databases (DB/DBX), and revocations for newly discovered boot-level vulnerabilities. Over time, this reduces protection against emerging boot-level threats but does not affect day-to-day functionality.

Customer Action Required

Action required	Reboot required	Service interruption	Compensating control
Yes	Yes	Brief	N/A

Affected Products

The following product families are within scope of this notice. See Material Lists at the end of this document for full CTN/SAP enumeration.

Product family / line	Affected versions
DIVAR IP all-in-one 6000 (DIP-64xx)	Initial production image with BIOS 2.1V3 version
DIVAR IP all-in-one 4000 (DIP-44xx)	Initial production image with BIOS 2.1V3 version

Notice

The DIVAR IP all-in-one 4000 (DIP-44xx) and DIVAR IP all-in-one 6000 (DIP-64xx) units manufactured after November 2024 with BIOS version 2.9a.V1 and 2.9.V1 respectively are not affected, as they already include Microsoft 2023 certificates.

The same applies to the DIVAR IP all-in-one 7000 (DIP-74xx) series.

Other currently in support DIVAR IP families, including DIVAR IP all-in-one 5000 (DIP-52xx), DIVAR IP all-in-one 7000 (DIP-72xx, DIP-73xx) are also not affected, as Secure Boot is not used on these models.

Technical Details

Considered Common Vulnerabilities and Exposures (CVE)

Not applicable. This notice covers a planned certificate lifecycle event, not a security vulnerability.

Issue Description

Microsoft is rotating the 2011-era Secure Boot certificates that anchor the UEFI trust chain on Windows devices. The Key Exchange Key (KEK) and UEFI CA certificates begin expiring in June 2026, followed by the Windows Production PCA in October 2026. Replacement 2023 certificates are being distributed through Windows Update and OEM firmware updates.

According to Microsoft, devices that have not received the 2023 certificates "will continue to start and operate normally" after the expiration dates, and standard Windows updates will keep installing. The functional impact is forward-looking: once the 2011 certificates expire, affected devices can no longer validate or install new early-boot artifacts signed under the new chain. This includes updates to the Windows Boot Manager, additions or revocations in the Secure Boot DB and DBX, and mitigations for boot-level vulnerabilities discovered after the expiration date. Existing boot components remain trusted and continue to load.

Devices not connected to the internet behave identically to the description above, they continue to boot and

operate normally. Any applicable Secure Boot updates are deferred until the device is next connected.

Why this affects IQSIGHT products

Affected DIP-44xx and DIP-64xx units manufactured with the initial production image carry the 2011 Microsoft Secure Boot certificate set in their UEFI firmware and have not received the 2023 certificates through subsequent firmware updates. After the June 2026 expiration, these units will continue to boot and run normally but will no longer receive new early-boot security updates. Day-to-day video management and recording functionality is unaffected. The BIOS/UEFI update listed in *Solutions and Mitigations* enrolls the 2023 certificates and restores the device's ability to receive future boot-level security updates.

Solutions and Mitigations

Upgrade the BIOS/UEFI to version 2.9a.V1 by following the procedure described in the SOP “*DIVAR IP all-in-one 4000 & 6000 BIOS Upgrade Guide*”, available at the link below.

- <https://fileshare.keenfinity-group.com/s/Ps3psrenctFMSzK>

The link also provides the required BIOS/UEFI update files:

- **DIP-44 BIOS_X12SCV-1B97-VV00020N00_20240516_2.9a.V1_OEMsp.bin** for upgrading DIVAR IP all-in-one 4000
- **DIP-64 BIOS_X12SCZ-F-1B6E-VV00020N00_20240705_2.9.V1_OEMsp.bin** for upgrading DIVAR IP all-in-one 6000

Warning

Applying the mitigation may require a system restart. Save any work and close all applications before rebooting. A reboot may result in a short video recording gap. Coordinate with operations before applying during business hours.

Notice

For consistent functionality, compatibility, performance, and security, keep firmware and software updated to the latest approved version throughout the device's operational life.

References

- <https://support.microsoft.com/en-gb/topic/windows-secure-boot-certificate-expiration-and-ca-updates-7ff40d33-95dc-4c3c-8725-a9b95457578e>

Material Lists

Complete enumeration of affected commercial product references.

Family name	CTN	SAP#	Material description
DIVAR IP all-in-one 6000	DIP-6440IG-00N	F.01U.404.045	Management appliance 1U w/o HDD
DIVAR IP all-in-one 6000	DIP-6444IG-4HD	F.01U.404.046	Management appliance 1U 4x4TB
DIVAR IP all-in-one 6000	DIP-6448IG-4HD	F.01U.404.047	Management appliance 1U 4x8TB
DIVAR IP all-in-one 6000	DIP-644IIG-4HD	F.01U.404.048	Management appliance 1U 4x18TB

Family name	CTN	SAP#	Material description
DIVAR IP all-in-one 4000	DIP-4420IG-00N	F.01U.404.040	Management appliance w/o HDD
DIVAR IP all-in-one 4000	DIP-4424IG-2HD	F.01U.404.041	Management appliance 2x4TB
DIVAR IP all-in-one 4000	DIP-4428IG-2HD	F.01U.404.042	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP-442IIG-2HD	F.01U.404.043	Management appliance 2x18TB

Document Change Log

Date	Version	Summary of changes
2026-06-26	1.0	Initial release.

© IQSIGHT. All rights reserved. This document is provided for informational purposes only. The information herein is subject to change without notice.