The impact of Android Verified Boot as a security feature in the latest ProDVX A26 firmware release

A26 is fully compliant with EU RED regulations

At ProDVX, security is at the heart of everything we do. This includes two firmware updates per year, that have the goal to protect your devices and data. With the latest A26 firmware release, we ensure that every device remains safe, reliable, and fully compliant with EU regulations.

To stay compliant with RED regulations, ProDVX implemented Verified Boot in this release. Read on discover it's benefits for secure devices, how it works and the risks that come with it once you downgrade this firmware to earlier firmware's.

How Verified Boot protects your devices

Verified Boot is a security mechanism that allows only verified and genuine ProDVX firmware to run.

- During startup, the device checks the firmware signature.
- The device only accepts so called signed firmware. Our A26 firmware release is signed, so accepted once the device starts. Unsigned, unsupported, or unsafe firmware cannot run and may render the device inoperable, preventing potential malware.
- New Android Panel PCs devices come with A26 firmware out of the box and include Verified Boot by default; existing devices can be updated to the A26 signed firmware using ProMGR.

Updating older devices:

- Devices that previously didn't have signed firmware, can typically run signed firmware safely, provided it is compatible with the hardware.
- Updates are subject to support status and technical limitations, so not all firmware may be available.

Scope and guidelines for updating ProDVX devices

- Verified Boot and signed firmware apply only to supported devices.
- Unsupported or end-of-life devices will not receive signed updates.
- Always use officially released, verified and genuine ProDVX firmware, and follow our upgrade guidelines.

Even for older devices, these measures are designed to protect your investment, prevent unauthorized firmware, and safeguard data, reflecting our commitment to security at every step.

Staying compliant with EU Radio Equipment Directive (RED)

The EU RED sets rules for safety, radio performance, and cybersecurity of all radio-enabled devices sold in the EU.

- It prevents devices from running unsafe or unauthorized firmware.
- It protects sensitive data, such as private or card information.
- Verified Boot is one of the measures ProDVX uses to meet RED cybersecurity requirements and device security. For this reason, Verified Boot is now part of the A26 firmware release.

Downgrading risks of A26 signed firmware to A25 (or earlier) unsigned firmware

Once a device runs signed firmware:

- Downgrading to unsigned firmware (A25 or lower) can permanently damage the device.
- Older unsigned firmware is only available on request through ProDVX support, because it comes with a risk for hardware with firmware that's already signed.
- ProDVX chooses mentioned changes in order to fulfill the EU RED regulations.

Verified Boot is a positive security feature, designed to prevent malware and keep your devices and data safe. But it comes with a risk which we need to be aware of.

Key takeaways

- Security is ProDVX's top priority, Verified Boot and signed firmware keep devices protected, stable, and RED-compliant.
- Always use verified and genuine ProDVX firmware.
- Contact ProDVX support before performing any updates or downgrades.