Verified Boot

Archived: 2026-04-02 12:41:39 UTC

Verified Boot strives to ensure all executed code comes from a trusted source (usually device OEMs), rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader, to the boot partition and other verified partitions including `system`, `vendor`, and optionally `oem` partitions. During device boot up, each stage verifies the integrity and authenticity of the next stage before handing over execution.

In addition to ensuring that devices are running a safe version of Android, Verified Boot checks for the correct version of Android with rollback protection. Rollback protection helps to prevent a possible exploit from becoming persistent by ensuring devices only update to newer versions of Android.

In addition to verifying the OS, Verified Boot also allows Android devices to communicate their state of integrity to the user.

Background

Android 4.4 added support for Verified Boot and the dm-verity kernel feature. This combination of verifying features served as Verified Boot 1.

Where previous versions of Android warned users about device corruption, but still allowed them to boot their devices, Android 7.0 started strictly enforcing Verified Boot to prevent compromised devices from booting. Android 7.0 also added support for forward error correction to improve reliability against non-malicious data corruption.

Android 8.0 and higher includes Android Verified Boot (AVB), a reference implementation of Verified Boot that works with Project Treble. In addition to working with Treble, AVB standardized partition footer format and added rollback protection features.

Source: https://source.android.com/security/verifiedboot/