

KR00K VULNERABILITY INFORMATION

Kr00k is a security vulnerability that allows some [WPA2](#) encrypted WiFi traffic to be decrypted. The vulnerability was originally discovered by security company [ESET](#) in 2019 and assigned [CVE-2019-15126](#) on August 17th, 2019.

The Kr00k vulnerability potentially affects all WiFi-capable devices that use WiFi chips made by Broadcom or Cypress.

We have carefully reviewed with the chipset vendors in respective devices. We confirm that the devices including PA700/720/726/730/760, EA600/500/502/602/EA510 and TB120/128/85/162/160 are safe to use without the threat of KR00K vulnerability. The models include [PA692](#) and [HT682](#) series are affected.

For HT682 and PA692, we are working solution to fix this problem. In the meantime, it's recommended that customers use TLS data encryption when possible as TLS tunneled data is not at risk for the kr00k vulnerability.