# CVE Detail – CVE-2021-3011

An electromagnetic-wave side-channel issue was discovered on NXP SmartMX / P5x security microcontrollers and A7x secure authentication microcontrollers, with CryptoLib through v2.9. It allows attackers to extract the ECDSA private key after extensive physical access (and consequently produce a clone). This was demonstrated on the Google Titan Security Key, based on an NXP A7005a chip. Other FIDO U2F security keys are also impacted (Yubico YubiKey Neo and Feitian K9, K13, K21, and K40) as well as several NXP JavaCard smartcards (J3A081, J2A081, J3A041, J3D145\_M59, J2D145\_M59, J3D120\_M60, J3D082\_M60, J2D120\_M60, J2D082\_M60, J3D081\_M59, J2D081\_M59, J3D081\_M61, J2D081\_M61, J3D081\_M59\_DF, J3D081\_M61\_DF, J3E081\_M64, J3E081\_M66, J2E081\_M64, J3E041\_M66, J3E016\_M66, J3E016\_M64, J3E041\_M64, J3E145\_M64, J3E120\_M65, J3E082\_M65, J2E145\_M64, J2E120\_M65, J2E082\_M65, J3E081\_M64\_DF, J3E081\_M66\_DF, J3E041\_M66\_DF, J3E016\_M66\_DF, J3E041\_M64\_DF, and J3E016\_M64\_DF).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.17614

## CVSS Scoring

CVSS v3.1 Score: 4.2

Severity: MEDIUM

## Mapped CWE(s)

* CWE-670: Always-Incorrect Control Flow Implementation

## Affected Products

* cpe:2.3:h:ftsafe:k13:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:ftsafe:k21:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:ftsafe:k40:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:ftsafe:k9:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:google:titan\_security\_key:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:3a081:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:a7005a:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2a081:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2d081\_m59:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2d081\_m61:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2d082\_m60:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2d120\_m60:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2d145\_m59:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2e081\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2e082\_m65:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2e120\_m65:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j2e145\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3a041:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d081\_m59:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d081\_m59\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d081\_m61:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d081\_m61\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d082\_m60:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d120\_m60:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3d145\_m59:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e016\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e016\_m64\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e016\_m66:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e016\_m66\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e041\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e041\_m64\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e041\_m66:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e041\_m66\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e081\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e081\_m64\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e081\_m66:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e081\_m66\_df:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e082\_m65:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e120\_m65:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:j3e145\_m64:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:p5010:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:p5020:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:p5021:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:nxp:p5040:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:yubico:yubikey\_neo:-:\*:\*:\*:\*:\*:\*:\*