Insufficient DPA countermeasure reseeding

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14972
State	PUBLISHED
Assigner	Silabs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 15:16:49 UTC
Updated	2026-05-18 20:27:23 UTC
Description	* Countermeasures for DPA within SYMCRYPTO engine on SixG301xxx devices are not sufficiently random and will eventu

Risk And Classification

Primary CVSS: v4.0 4.1 MEDIUM from product-security@silabs.com

CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000180000 probability, percentile 0.050570000 (date 2026-05-18)

Problem Types: CWE-331 | CWE-331 CWE-331 Insufficient entropy

Version	Source	Type	Score	Severity	Vector
4.0	product-security@silabs.com	Secondary	4.1	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/
4.0	CNA	CVSS	4.1	MEDIUM	CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Silabs.com	Simplicity SDK	affected *.* semver	Not specified

References

Reference	Source	Link	Tags
community.silabs.com/068Vm00000M3cAX	product-security@silabs.com	community.silabs.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.