



# Insufficient DPA countermeasure reseeding

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

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

## 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/MSX/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

Integrity

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/MSX/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	<a href="https://silabs.com">Silabs.com</a>	Simplicity SDK	affected *.* semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://community.silabs.com/068Vm00000M3cAX">community.silabs.com/068Vm00000M3cAX</a>	<a href="mailto:product-security@silabs.com">product-security@silabs.com</a>	<a href="https://community.silabs.com">community.silabs.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)