Timing limitations of the HRNG in RS9116 when power save mode is enabled results in predictable values

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

Summary

CVE	CVE-2026-3290
State	PUBLISHED
Assigner	Silabs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 20:17:04 UTC
Updated	2026-05-15 14:11:57 UTC
Description	Timing limitations of the HRNG in RS9116 when power save mode is enabled results in predictable values

Risk And Classification

Primary CVSS: v4.0 7.4 HIGH from product-security@silabs.com

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/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

Problem Types: CWE-332 | CWE-332 CWE-332

Version	Source	Type	Score	Severity	Vector
4.0	product-security@silabs.com	Secondary	7.4	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	7.4	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/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	Silicon Labs	RS9116 SDK	affected 2.13.1 semver	Not specified

References

Reference	Source	Link
github.com/SiliconLabs/wiseconnect-wifi-bt-sdk	product-security@silabs.com	github.com
siliconlabs.lightning.force.com/sfc/servlet.shepherd/document/download/069Vm00000nIg6IIAS	product-security@silabs.com	siliconlabs.lig
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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