crypto: ATAES132A response length allows stack buffer overflow

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-0849
State	PUBLISHED
Assigner	zephyr
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-16 14:18:07 UTC
Updated	2026-04-02 14:26:59 UTC
Description	Malformed ATAES132A responses with an oversized length field overflow a 52-byte stack buffer in the Zephyr crypto driver

Risk And Classification

Primary CVSS: v3.1 6.8 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-120 | CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	vulnerabilities@zephyrproject.org	Secondary	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Zephyrproject	Zephyr	4.3.0	-	All	All
Operating System	Zephyrproject	Zephyr	4.3.0	rc1	All	All
Operating System	Zephyrproject	Zephyr	4.3.0	rc2	All	All
Operating System	Zephyrproject	Zephyr	4.3.0	rc3	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zephyrproject-rtos	Zephyr	affected * 4.3 git	Not specified

References

Reference	Source	Link	Ta
github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-ff4p-3ggg-...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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