



CVE-2026-25205

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-25205
State	PUBLISHED
Assigner	samsung.tv_appliance
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 05:16:02 UTC
Updated	2026-04-13 15:01:43 UTC
Description	Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows out-of-bounds write. This issue affects E

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from PSIRT@samsung.com

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

EPSS: 0.000130000 probability, percentile 0.020910000 (date 2026-04-15)

Problem Types: CWE-122 | CWE-122 CWE-122 Heap-based buffer overflow

Version	Source	Type	Score	Severity	Vector
3.1	PSIRT@samsung.com	Secondary	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Samsung Open Source	Escargot	affected 97e8115ab1110bc502b4b5e4a0c689a71520d335	Not specified

References

Reference	Source	Link	Tags
github.com/Samsung/escargot/pull/1554	PSIRT@samsung.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Sebastián Alba Vives / @Sebasteuo (en)

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report