



# Ember ZNet buffer overflow in 'packet handoff' plugin

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

## Summary

<b>CVE</b>	CVE-2024-10106
<b>State</b>	PUBLISHED
<b>Assigner</b>	Silabs
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-01-09 15:15:12 UTC
<b>Updated</b>	2026-04-16 20:16:36 UTC
<b>Description</b>	A buffer overflow vulnerability in the packet handoff plugin allows an attacker to overwrite memory outside the plugin's buffer.

## Risk And Classification

**Primary CVSS:** v3.1 3.7 LOW from product-security@silabs.com

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

**EPSS:** 0.002910000 probability, percentile 0.525390000 (date 2026-04-16)

**Problem Types:** cwe-120

Version	Source	Type	Score	Severity	Vector
3.1	product-security@silabs.com	Secondary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	<a href="https://silabs.com">Silabs.com</a>	Ember ZNet SDK	affected 8.0.0 8.0.2 semver	Not specified
CNA	<a href="https://silabs.com">Silabs.com</a>	Ember ZNet SDK	affected 7.3.0 7.4.4 semver	Not specified
CNA	<a href="https://silabs.com">Silabs.com</a>	Ember ZNet SDK	affected 7.2.6 semver	Not specified

References			
Reference	Source	Link	Tags
<a href="https://community.silabs.com/069Vm0000011JawIAF">community.silabs.com/069Vm0000011JawIAF</a>	product-security@silabs.com	<a href="https://community.silabs.com">community.silabs.com</a>	
<a href="https://github.com/SiliconLabs/simplicity_sdk/releases">github.com/SiliconLabs/simplicity_sdk/releases</a>	product-security@silabs.com	<a href="https://github.com">github.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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**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)