



# CVE-2026-28815

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

## Summary

<b>CVE</b>	CVE-2026-28815
<b>State</b>	PUBLISHED
<b>Assigner</b>	apple
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-03 03:16:18 UTC
<b>Updated</b>	2026-04-03 03:16:18 UTC
<b>Description</b>	A remote attacker can supply a short X-Wing HPKE encapsulated key and trigger an out-of-bounds read in the C decapsulation

## Risk And Classification

**Problem Types:** A remote attacker can supply a short X-Wing HPKE encapsulated key and trigger an out-of-bounds read in the C decapsulation path, potentially causing a crash or memory disclosure depending on runtime protections.

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Apple</a>	<a href="#">MacOS</a>	affected 4.0.0 4.3.1 custom	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/apple/swift-crypto/security/advisories/GHSA-9m44-rr2w-ppp7">github.com/apple/swift-crypto/security/advisories/GHSA-9m44-rr2w-ppp7</a>	product-security@apple.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.

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**