CVE-2026-28815

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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	Apple	MacOS	affected 4.0.0 4.3.1 custom	Not specified

References

Reference	Source	Link	Tags
github.com/apple/swift-crypto/security/advisories/GHSA-9m44-rr2w-ppp7	product-security@apple.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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