

CVE-2026-65400

Apple macOS Improper Authentication Vulnerability

CISA KEV since Aug 18, 2026

Actively exploited

An authentication issue was addressed with improved state management. This issue is fixed in macOS Golden Gate 27, macOS Sequoia 15.7.9, macOS Sonoma 14.8.9, macOS Tahoe 26.6.1, macOS Tahoe 26.7. An attacker on the network may be able to authenticate to Screen Sharing without valid credentials.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.017 77.3rd percentile · FIRST	CISA DEADLINE Aug 21, 2026 CISA federal deadline · Overdue by 2 months
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.017 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
macos	≥ 14.0 < 14.8.9 ≥ 15.0 < 15.7.9 ≥ 26.0 < 26.6.1	14.8.9 · 15.7.9 · 26.6.1	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-cwph-f4w9-f4wq	support.apple.com	support.apple.com/en-us/148170
support.apple.com	support.apple.com/en-us/148171	support.apple.com	support.apple.com/en-us/148172
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-65400	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-54216	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-65400

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.