

Apple CoreGraphics Out-of-Bounds Write Vulnerability Affects iOS, macOS and iPadOS



Apple has disclosed an out-of-bounds write vulnerability in CoreGraphics affecting iOS, macOS and iPadOS that may enable arbitrary code execution.

- CVE-2026-86950 is an out-of-bounds write vulnerability in Apple CoreGraphics component
- Affects iOS, macOS and iPadOS across multiple Apple products
- Successful exploitation may lead to arbitrary code execution
- CISA recommends applying vendor mitigations and evaluating internet-exposed assets
- Organisations should discontinue use if mitigations are unavailable

Vulnerability Overview

Apple has disclosed **CVE-2026-86950**, an out-of-bounds write vulnerability affecting the CoreGraphics component in iOS, macOS and iPadOS. This class of vulnerability occurs when software writes data beyond the boundaries of allocated memory buffers, potentially allowing attackers to execute arbitrary code on affected devices. The flaw poses a significant risk to organisations relying on Apple devices for business operations.

Risk and Exposure

Successful exploitation of this vulnerability may lead to **arbitrary code execution**, enabling attackers to run malicious code with the privileges of the affected application or system component. For regulated institutions in the Kingdom, this presents particular concern where Apple devices are used to access sensitive systems, customer data or critical infrastructure. The US Cybersecurity and Infrastructure Security Agency has issued guidance recommending organisations apply vendor mitigations and evaluate each asset's internet exposure.

Recommended Response

Organisations should prioritise applying security updates in accordance with Apple's vendor instructions. CISA guidance emphasises the importance of risk-based patching and forensic triage requirements. Where mitigations are not available or cannot be applied in a timely manner, institutions should consider discontinuing use of affected products until patches are released. Cloud service deployments require particular attention to ensure applicable patching guidelines are followed across all environments.

What to do now

1. Inventory all Apple iOS, macOS and iPadOS devices across the institution and cloud environments
2. Apply security updates from Apple immediately in accordance with vendor instructions
3. Evaluate internet exposure of each affected asset and prioritise patching based on risk
4. Review and implement forensic triage requirements for affected systems
5. Discontinue use of affected products where mitigations cannot be applied in a timely manner
6. Document patching activities and compliance with internal change management procedures