

# CVE-2022-32917

## Apple iOS, iPadOS, and macOS Remote Code Execution Vulnerability

CISA KEV since Sep 14, 2022

Actively exploited

The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited..

|                                                       |                                       |                                                   |                                                                            |
|-------------------------------------------------------|---------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------|
| EVRS<br><b>75</b> / <sub>100</sub><br>Urgent priority | CVSS V3.1<br><b>7.8</b><br>High · NVD | EPSS<br><b>0.056</b><br>92.9th percentile · FIRST | CISA DEADLINE<br><b>Oct 5, 2022</b><br>KEV since 2022 · listed over a year |
|-------------------------------------------------------|---------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.056 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 7.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE   | AFFECTED                         | FIXED IN    | SOURCE |
|-----------|----------------------------------|-------------|--------|
| ipados    | < 15.7                           | 15.7        | NVD    |
| iphone os | < 15.7                           | 15.7        | NVD    |
| macos     | ≥ 11.0 < 11.7<br>≥ 12.0.0 < 12.6 | 11.7 · 12.6 | NVD    |

### Sources

|                          |                                                                                                                                                                                           |                            |                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b>   | <a href="https://github.com/advisories/GHSA-fffx-3h8f-f943">github.com/advisories/GHSA-fffx-3h8f-f943</a>                                                                                 | <b>Additional guidance</b> | <a href="https://support.apple.com/en-us/HT213443">support.apple.com/en-us/HT213443</a>                                     |
| <b>support.apple.com</b> | <a href="https://support.apple.com/en-us/HT213445">support.apple.com/en-us/HT213445</a> , <a href="https://support.apple.com/en-us/HT213444">https://support.apple.com/en-us/HT213444</a> | <b>NVD</b>                 | <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-32917">nvd.nist.gov/vuln/detail/CVE-2022-32917</a>                       |
| <b>CISA KEV</b>          | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                   | <b>ENISA EUVD</b>          | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2022-35983">euvd.enisa.europa.eu/vulnerability/EUVD-2022-35983</a> |
| <b>Current data</b>      | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2022-32917">evulnable.com/vulnerability-management/cve/CVE-2022-32917</a>                                                 |                            |                                                                                                                             |

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