

# CVE-2021-30761

## Apple iOS WebKit Memory Corruption Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.5.4. Processing maliciously crafted web content may lead to arbitrary code execution. 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>8.8</b><br>High · NVD | EPSS<br><b>0.105</b><br>95.8th percentile · FIRST | CISA DEADLINE<br><b>Nov 17, 2021</b><br>KEV since 2021 · 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>     | 0.105 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 8.8                           | <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 |
|-----------|----------|-------------------------|--------|
| iphone os | < 12.5.4 | no fixed version listed | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-6qp6-2ggr-xv6x](https://github.com/advisories/GHSA-6qp6-2ggr-xv6x)  
**NVD** [nvd.nist.gov/vuln/detail/CVE-2021-30761](https://nvd.nist.gov/vuln/detail/CVE-2021-30761)**Additional guidance** [support.apple.com/en-us/HT212548](https://support.apple.com/en-us/HT212548)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)  
**Current data** [evulnable.com/vulnerability-management/cve/CVE-2021-30761](https://evulnable.com/vulnerability-management/cve/CVE-2021-30761)**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2021-17678](https://euvd.enisa.europa.eu/vulnerability/EUVD-2021-17678)

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