# CVE Detail – CVE-2021-1879

This issue was addressed by improved management of object lifetimes. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3. Processing maliciously crafted web content may lead to universal cross site scripting. Apple is aware of a report that this issue may have been actively exploited..

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.83091

## CVSS Scoring

CVSS v3.1 Score: 6.1

Severity: MEDIUM

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## CAPEC(s)

* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-588: DOM-Based XSS
* CAPEC-591: Reflected XSS
* CAPEC-592: Stored XSS
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-85: AJAX Footprinting

## Affected Products

* cpe:2.3:o:apple:ipados:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:iphone\_os:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:iphone\_os:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:watchos:\*:\*:\*:\*:\*:\*:\*:\*