

Multiple Vulnerabilities in Apple Products

A. Description:

1. Arbitrary Code Execution Vulnerability (CVE-2024-44308)

This vulnerability exists in JavaScriptCore, which is used by Apple's Safari browser and other applications to process JavaScript. An attacker could exploit this issue to execute arbitrary code execution by sending maliciously crafted web content to the affected device.

2. Cross-Site Scripting Vulnerability (CVE-2024-44309)

The vulnerability exists in WebKit, the engine that powers Safari and web content on Apple devices. An attacker could exploit this issue by sending maliciously crafted web content to trigger cross-site scripting (XSS) on the affected device.

Note: These vulnerabilities may have been actively exploited on Intel-based Mac systems. Users are strongly advised to update their devices to the latest software versions to mitigate the risk.

B. CVE IDs, Affected Products and Solution:

CVE	Affected Products	Solutions
CVE-2024-44308 CVE-2024-44309	<ul style="list-style-type: none">Apple iOS and iPadOS versions prior to 18.1.1Apple iOS and iPadOS versions prior to 17.7.2Apple macOS Sequoia versions prior to 15.1.1Apple visionOS versions prior to 2.1.1Apple Safari versions prior to 18.1.1	Apply appropriate security updates mentioned in the Apple Security Updates: https://support.apple.com/en-us/121

C. References:

1. <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2024-0058>
2. <https://support.apple.com/en-us/121753>

Disclaimer- The information provided herein is on "as is" basis, without warranty of any kind.