

No.10 (6)/2016-Coord  
Government of Pakistan  
Ministry of Science and Technology  
\*\*\*\*\*

Islamabad, the 19<sup>th</sup> May, 2025

Subject: **CYBER SECURITY ADVISORY-APPLE PATCHES ACTIVELY  
EXPLOITED WEBKIT ZERO-DAY (ADVISORY NO. 08/2025)**

Enclosed please find herewith Cabinet Division's U.O No.1-5/2023/24(NTISB-II) dated 16<sup>th</sup> May, 2025 on the subject cited above. The content of the letter is reproduced under for strict compliance, please.

**Context.** Apple has released critical security updates addressing a zero-day vulnerability (CVE-2025-24201) in the WebKit browser engine. This vulnerability has been exploited in targeted attacks to execute unauthorized actions on affected devices. The flaw was initially discovered in iOS 17.2 but has now been identified in later versions, prompting urgent updates across iOS, macOS and visionOS.

2. **Technical Details**

a. **Vulnerabilities ID.** CVE-2025-24201

b. **Impact.** Exploiting this flaw allows Critical authentication bypass the Web Content sandbox, potentially enabling arbitrary code execution

c. **Affected Systems**

(1) **iOS & iPadOS.** iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch (3<sup>rd</sup> gen and later), iPad Air (3<sup>rd</sup> gen and later), iPad mini (5<sup>th</sup> gen and later).

(2) **macOS.** Sequoia 15.3.2, macOS Ventura & Sonoma (Safari update required).

(3) **visionOS.** Apple Vision Pro (requires visionOS 2.3.2 update).

d. **Attack Vector.** Web-based exploitation through malicious websites, making users vulnerable if they visit infected pages using Safari or apps utilizing Webkit.

3. **Recommendations.** All apple users are urged to immediately update to following versions and enable automatic updates to receive future security patches without delay:

a. **iOS & iPadOS.** Install iOS 18.3.2/iPadOS 18.3.2

b. **macOS.** Update Sequoia to 15.3.2, or update Safari for Ventura & Sonoma

c. **visionOS.** Upgrade to visionOS 2.3.2

2. This message is to all concerned in your organization for ensuring necessary protective measures, Please.

Encl: As above.

  
(RIDA NOOR)  
Section Officer (Coord)  
Tel: 9202520

**Distribution:**

All Head of Organizations

**Copy for information to:**

All Heads of Wing, MoST





GOVERNMENT OF PAKISTAN  
CABINET DIVISION

\*\*\*\*\*



**SUBJECT: CYBER SECURITY ADVISORY-APPLE PATCHES ACTIVELY EXPLOITED WEBKIT ZERO-DAY (ADVISORY NO. 08/2025)**

**Context.** Apple has released critical security updates addressing a zero-day vulnerability (CVE-2025-24201) in the WebKit browser engine. This vulnerability has been exploited in targeted attacks to execute unauthorized actions on affected devices. The flaw was initially discovered in iOS 17.2 but has now been identified in later versions, prompting urgent updates across iOS, macOS and visionOS.

2. **Technical Details**

a. **Vulnerabilities ID.** CVE-2025-24201

b. **Impact.** Exploiting this flaw allows Critical authentication bypass the Web Content sandbox, potentially enabling arbitrary code execution

c. **Affected Systems**

(1) **iOS & iPadOS.** iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch (3<sup>rd</sup> gen and later), iPad Air (3<sup>rd</sup> gen and later), iPad mini (5<sup>th</sup> gen and later).

(2) **macOS.** Sequoia 15.3.2, macOS Ventura & Sonoma (Safari update required).

(3) **visionOS.** Apple Vision Pro (requires visionOS 2.3.2 update).

d. **Attack Vector.** Web-based exploitation through malicious websites, making users vulnerable if they visit infected pages using Safari or apps utilizing Webkit.

3. **Recommendations.** All apple users are urged to immediately update to following versions and enable automatic updates to receive future security patches without delay:

a. **iOS & iPadOS.** Install iOS 18.3.2/iPadOS 18.3.2

b. **macOS.** Update Sequoia to 15.3.2, or update Safari for Ventura & Sonoma

c. **visionOS.** Upgrade to visionOS 2.3.2

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

**Major Hafiz Adnan Rana**  
**Assistant Secretary NTISB-II**



Central Registry NUTECH	
✓ Rector	CM
Pro-Rector	
Dy Dir (Coord)	
GSO-1 (Coord)	Q
Head Clk	Ami
Dte/Office	ICT
Diary No	
Date	20/5/25

ICT  
share with  
all

Rida Noor  
Section Officer Coordination  
16 May , 2025, 03:39:31 PM