Mobile app agent

Mobile security, device management and BYOD consent

01 Overview | 02 Assets | 03 Intelligence | 04 Actions

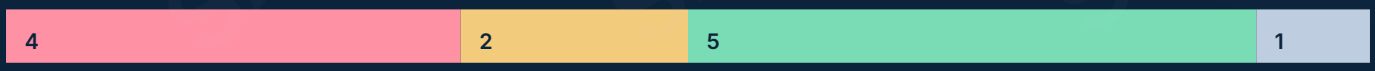
Action required

Update two iPhones and complete the lost-device response.

An iOS security flaw affects two devices. A separate lost-device incident remains open.

12	4	1	1
Devices in scope	High-priority assets	Known vulnerabilities	Overdue actions

ASSET STATUS



4 Action | 2 Attention | 5 Pass | 1 Unknown

SECURITY CHECKS

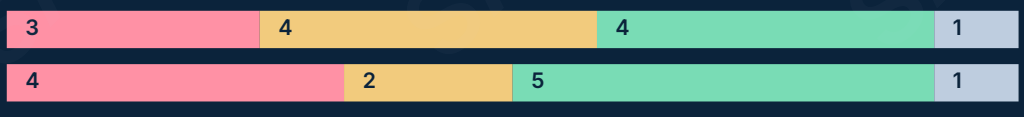
MDM	10/12 pass
Encryption	11/12 pass
Screen lock	10/12 pass
OS posture	8/12 pass
Consent	3/4 pass

Assessment coverage: 48 of 52 applicable checks returned a result. Grey indicates missing or outdated evidence.

TOP THREE PRIORITIES

1	**Update two iOS devices**	Mobile administrator / 12 Sep
2	**Investigate the jailbreak alert**	Security operations / 13 Sep
3	**Complete the lost-device response**	Security operations / 13 Sep

CHANGE SINCE 06 SEPTEMBER



2 checks now pass; one new issue. Both assessments cover the same assets.

12 mobile devices | 8 iOS + 4 Android | 4 BYOD owners | Microsoft Intune

Asset security overview

Security checks for each asset, ordered by priority.

01 Overview | 02 Assets | 03 Intelligence | 04 Actions

! Action ! Attention + Pass ? Unknown

ASSET / PLATFORM	MDM	Encryption	Screen lock	OS posture	Consent
MOB-01 iOS	+ Pass	+ Pass	+ Pass	! Action	- N/A
MOB-02 iOS	+ Pass	+ Pass	+ Pass	! Action	- N/A
MOB-11 Android	+ Pass	+ Pass	+ Pass	! Action	- N/A
MOB-12 Android	! Action	+ Pass	+ Pass	+ Pass	- N/A
MOB-09 Android	+ Pass	+ Pass	! Attention	+ Pass	+ Pass
MOB-10 Android	+ Pass	+ Pass	+ Pass	+ Pass	! Attention
MOB-08 iOS	? Unknown	? Unknown	? Unknown	? Unknown	- N/A
MOB-03 iOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
MOB-04 iOS	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
MOB-05 iOS	+ Pass	+ Pass	+ Pass	+ Pass	- N/A
MOB-06 iOS	+ Pass	+ Pass	+ Pass	+ Pass	- N/A
MOB-07 iOS	+ Pass	+ Pass	+ Pass	+ Pass	- N/A

N/A checks are excluded from totals. Grey indicates missing or outdated evidence. Software checks do not cover every published vulnerability.

LOST-DEVICE RESPONSE

1 **Reported**
12 Sep 14:00

2 **Tokens revoked**
14:20

3 **Wipe requested**
14:25

4 **Completion**
Not verified

The incident remains open while wipe completion is unconfirmed.

Vulnerabilities and updates

Affected versions, exploitation status and recommended updates.

Affected version confirmed

CVE-2023-41993

Apple iOS / WebKit

Malicious web content may allow an attacker to run code on the device.

8.8	YES	29.18%	2
CVSS 3.1	Known exploitation (KEV)	30-day likelihood	Affected devices

INSTALLED VERSION	ORIGINAL FIX VERSION
17.0	17.0.1 (iOS 17)

Affected versions: iOS 17.0 is affected; the iOS 17 fix was released in 17.0.1
Evidence: Device management records identify Apple iOS 17.0.

RECOMMENDED UPDATE

Install the latest supported iOS update available for each device. Confirm the new version in the device management system.

The original fix version is historical. Use the latest supported release.

Affected assets: MOB-01, MOB-02
Scope: 1 vulnerability across 2 assets. This report includes selected CVE examples.

Source dates: EPSS 2026-09-12; CISA KEV 2026-09-11; NVD updated 2026-06-17.
EPSS estimates the chance of this vulnerability being exploited in the next 30 days. It does not predict a breach of your organisation. EPSS percentile: 98.06%.

NVD record | Apple security advisory | EPSS explained | CISA KEV

Remediation plan

Actions, responsible teams, deadlines and verification.

01 Overview | 02 Assets | 03 Intelligence | 04 Actions

6	1	2
Open actions	Overdue	Checks now passing

01 Update two iOS devices — OVERDUE 12 Sep

Install the supported update recommended on page 3 and confirm the version in use.

MOB-F01 | Mobile administrator | 2 assets | Open

02 Investigate the jailbreak alert — DUE 13 Sep

Investigate the jailbreak alert and apply the required corporate access restrictions.

MOB-F02 | Security operations | 1 asset | Open

03 Complete the lost-device response — DUE 13 Sep

Confirm the device management service has completed the requested response and finish the incident actions.

MOB-F03 | Security operations | 1 asset | Open

04 Renew BYOD consent — DUE 16 Sep

Obtain consent to the current BYOD policy before enabling data collection that requires consent.

MOB-F04 | BYOD reviewer | 1 asset | Open

05 Apply the screen-lock policy — DUE 16 Sep

Apply the required screen-lock timeout and confirm the setting on the device.

MOB-F05 | Mobile administrator | 1 asset | Open

06 Restore device synchronisation — DUE 14 Sep

Restore synchronisation with the device management service and collect an updated security report.

MOB-F06 | Mobile administrator | 1 asset | Open

Lost-device response: reported 12 Sep at 14:00; tokens revoked at 14:20; wipe requested at 14:25. **Wipe completion is unconfirmed.** The incident remains open.