Google patches critical Android flaw allowing remote code execution without user action



Google's November bulletin fixes CVE-2026-58868, a critical Android 14–17 flaw that could let an attacker run code remotely with no user action. The fix arrives with patch level 2026-11-01 or later.

- The flaw is tracked as CVE-2026-58868 and rated critical by Google.
- It could allow remote code execution on a phone without any user interaction.
- Android versions 14 through 17 are affected.
- The fix is included in security patch level 2026-11-01 or later.
- Phone makers and carriers release updates on their own schedules, so availability will vary by device.

Google has disclosed a critical Android vulnerability in its November security bulletin. Tracked as CVE-2026-58868, the flaw could allow an attacker to run code on a phone remotely, without the user taking any action.

What is affected

The issue affects Android 14 through 17. Google has addressed it in security patch level 2026-11-01 or later. Phone makers and carriers distribute these updates on their own schedules, so some devices will receive the fix later than others. The source, dated as of November 4, notes the state of the bulletin at that point, and the text available to us does not go further on exploitation details.

Why it matters for regulated institutions

A flaw that needs no user interaction removes the usual protection of staff awareness. Mobile devices used for email, banking applications, multi-factor authentication and approvals are a realistic route into institutional data if left unpatched. The practical exposure depends on how quickly each device model receives the update.

Recommended approach

Treat this as a priority patching item for the mobile fleet. Establish which devices run Android 14 to 17, check their current patch level, and confirm with your device vendors or carriers when the 2026-11-01 update will be available. Where updates are delayed, consider temporary restrictions on access to sensitive systems from unpatched devices until they are updated.

What to do now

1. Inventory managed and BYOD Android devices running versions 14 to 17.
2. Check each device's security patch level and flag those below 2026-11-01.
3. Ask device vendors and carriers for the release date of the November update for your models.
4. Push the update through your MDM as soon as it is available and track compliance.
5. Restrict unpatched devices from accessing sensitive applications until updated.