Google issues emergency Chrome update for eighth zero-day exploited this year



Google has released emergency updates for a Chrome vulnerability already exploited in attacks, the eighth Chrome zero-day patched since the start of the year. The source excerpt gives no further technical detail.

- Google shipped emergency security updates for Chrome.
- The flaw was exploited in zero-day attacks before the fix.
- It is the eighth Chrome zero-day patched since the start of the year.
- The available source text does not give a CVE number, affected versions or attack details.

Google has released emergency security updates for Chrome to fix a vulnerability that attackers were already exploiting. According to the report, this is the eighth Chrome zero-day patched since the start of the year.

What is known

The source excerpt confirms only the essentials: the update is an emergency release, the flaw was exploited in real attacks, and it is the eighth of its kind this year. It does not provide a CVE identifier, the affected or fixed version numbers, or details of who was targeted. We have therefore not included any of these.

Why it matters

Browsers are used on almost every managed endpoint, and a vulnerability that is exploited before a patch exists leaves little time for preparation. A steady pace of such flaws makes fast, routine browser patching a basic control rather than an occasional task.

What to do next

Check Google's official release notes for the exact version and CVE details, then confirm that managed Chrome installations have received the update. Organisations that rely on Chromium-based browsers should also watch for vendor guidance, but only act on confirmed information.

What to do now

1. Verify in Google's official release notes the fixed Chrome version and any CVE identifier.
2. Confirm that all managed desktops have updated Chrome and restart the browser where required.
3. Check patch-management reports for endpoints that have not yet updated, and follow up on them.
4. Review the browser patching timeline in your vulnerability management process for actively exploited flaws.
5. Monitor vendor advisories for Chromium-based browsers used in the organisation.