ChromeOS LTS-150 (Chrome) use-after-free and other security fixes (CVE-2026-125350)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:29 AM PST · Google's estimate: Fixed versions are available

CVE-2026-87626, CVE-2026-121135, CVE-2026-103627, CVE-2026-131023, CVE-2026-126921, CVE-2026-126890, CVE-2026-126886, CVE-2026-126852, CVE-2026-126892, CVE-2026-125350, CVE-2026-126840, CVE-2026-126854, CVE-2026-131101, CVE-2026-126851, CVE-2026-130952, CVE-2026-126913, CVE-2026-91731, CVE-2026-93385, CVE-2026-106393, CVE-2026-121184 · CVSS 8.8 (high) · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

Google is rolling out ChromeOS LTS-150 version 150.0.7871.290 (platform version 16700.71.0) to most ChromeOS devices on the Long-term Support channel. It was announced November 27, 2026 and includes selected security fixes for many Chrome flaws, such as memory-handling bugs (use-after-free and out-of-bounds read). One of the CVEs, CVE-2026-125350, is a high-severity use-after-free bug in Chrome's XML handling. Google first fixed it in regular Chrome on November 9, 2026, and says it is being exploited. News reports describe a CVSS score of 8.8 (a 0–10 severity scale), and we did not check this score against NVD. A use-after-free is a bug where a program keeps using memory after it has been released, which attackers can sometimes use to run their own code. According to CVE.org's description as quoted by The Hacker News, an attacker could run code inside the browser's protective sandbox through a specially crafted web page. Only some of the vulnerabilities listed are known to be exploited, and the fixes are bundled together in this one update.

WHO IS AFFECTED

- ChromeOS devices on the Long-term Support (LTS) channel running LTS-150 versions earlier than 150.0.7871.290
- Managed Chromebooks, such as those used by schools and businesses, that are set to the LTS channel
- Regular Google Chrome on Windows, Mac and Linux earlier than the fixed release, for CVE-2026-125350. News reports cite Chrome 157.0.8103.50 or later as the fix. Check Google's Chrome release notes for the exact version for your platform.
- Other Chromium-based browsers, such as Microsoft Edge and Opera, may also be affected, according to CISA's entry as reported by news outlets. Check each vendor for its own update.

IS IT BEING EXPLOITED?

CISA added CVE-2026-125350 (Google Chromium use-after-free) to its Known Exploited Vulnerabilities catalog on November 10, 2026. Google said it is aware that an exploit exists in the wild. Only this one CVE is confirmed as exploited. We have not confirmed that the other CVEs in the LTS-150 update are being exploited. Details on how it is being abused, or by whom, have not been published.

WHAT YOU SHOULD DO NOW

Home users

- Most home Chromebooks are on the Stable channel, not LTS. Update them anyway: open Settings > About ChromeOS > Check for updates, then restart when prompted.
- On a computer, update Chrome: open the three-dot menu > Help > About Google Chrome. Chrome will download the update, and you then click Relaunch.
- If you use Microsoft Edge, Opera, Brave or another Chromium-based browser, open its About page and install any available update.

• Restart your device or browser after updating. Updates do not take effect until you restart.
• Until you have updated, be careful with links and websites from unknown sources.

Businesses

• In the Google Admin console, go to Devices > Chrome > Settings > Device settings, find the Auto-update settings, and confirm which release channel each organizational unit uses.
• For devices on LTS, confirm they receive 150.0.7871.290. Go to Devices > Chrome > Devices and sort or filter by OS version to find any device still below that version.
• Devices must be on, or pinned to, a ChromeOS version no later than the LTS version to receive it. Review any version pinning that may be holding devices back.
• Have users restart Chromebooks that have downloaded the update but not yet rebooted.
• Update Chrome and other Chromium-based browsers on Windows, Mac and Linux computers. Use your normal software management tools to verify the installed versions.
• CISA's required deadline for US federal agencies to patch CVE-2026-125350 was November 24, 2026. Private organizations are not bound by it, but it is a useful benchmark for urgency.

HOW TO CHECK IF YOU'RE AFFECTED

• On a Chromebook: open Settings > About ChromeOS > Additional details. Look at the Version line. On the LTS channel the version should be 150.0.7871.290 or later.
• In Chrome on a computer: open the three-dot menu > Help > About Google Chrome. Compare the version number with the one listed in Google's Chrome Releases notes.
• For managed devices: in the Google Admin console, open Devices > Chrome > Devices and check the OS version column.

FIXED VERSIONS AND WORKAROUNDS

• ChromeOS LTS-150: 150.0.7871.290 (platform version 16700.71.0)
• Google Chrome (desktop), for CVE-2026-125350: Reported by news outlets as 157.0.8103.50 or later. Confirm in Google's Chrome release notes.

Until you can update:

• No workaround has been published. Installing the update is the fix.
• Until devices are updated, avoid opening untrusted links or websites on them.

OFFICIAL SOURCES

Chrome Releases: Long Term Support Channel Update for ChromeOS (LTS-150, November 27, 2026) — https://chromereleases.googleblog.com/2026/11/long-term-support-channel-update-for_01009121915.html
CISA Adds Six Known Exploited Vulnerabilities to Catalog (November 10, 2026) — https://www.cisa.gov/news-events/alerts/2026/11/10/cisa-adds-six-known-exploited-vulnerabilities-catalog
Long-term Support (LTS) on ChromeOS - Chrome Enterprise and Education Help — https://support.google.com/chrome/a/answer/11333726?hl=en

OTHER COVERAGE

The Hacker News: Google Issues Chrome Security Update for Eighth Actively Exploited Zero-Day of 2026 — https://thehackernews.com/2026/11/google-issues-chrome-security-update.html
Australian Cyber Security Magazine: Australian researcher credited for reporting exploited Chrome flaw in 27-year-old code — https://australiancybersecuritymagazine.com.au/australian-researcher-credited-for-reporting-exploited-chrome-flaw-in-27-year-old-code/
AboutChromebooks: ChromeOS LTS-150 Update Patches Six Critical Security Flaws On Long-Term Support Chromebooks — https://www.aboutchromebooks.com/chromeos-lts-150-update-patches-six-critical-security-flaws-on-long-term-support-chromebooks/

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.

Questions? Contact BIS Computer Solutions, Inc.
5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com