Threat Brief

Updated Sep 6, 2026 - 1:18 AM EDT - askanything-app.com

ACTIVELY EXPLOITED

Google patches Chrome's 6th actively-exploited zero-day of 2026 - CISA gives federal agencies until Sept 18

WHAT HAPPENED

Google shipped an emergency Chrome update after confirming in-the-wild exploitation of a V8 type-confusion bug that lets malicious web content corrupt memory and achieve code execution inside the sandbox. CISA added it to KEV within hours of disclosure.

AFFECTED

Google Chrome before 152.0.7977.82/.83 (Windows/macOS) and before 152.0.7977.82 (Linux); the same release also fixes 11 other bugs (10 high, 2 medium) in V8, WebGL, Skia, Network, and DevTools.

EXPLOITATION

Actively exploited in the wild - confirmed by Google; reported to Google by researcher Salvatore Gulizia. CISA KEV remediation due date: 2026-09-18 for federal civilian agencies.

FIX

Update to Chrome 152.0.7977.82/.83 or later (and the equivalent Chromium-based browser builds - Edge, Brave, etc. - once they ship).

CHECK IF YOU'RE EXPOSED

Check `chrome://version` on managed fleets; anything reporting a build below 152.0.7977.82 is vulnerable. Force an update push via your browser-management policy rather than waiting for auto-update.

SOURCE

[Help Net Security - Google patches actively exploited Chrome zero-day (CVE-2026-85046)](https://www.helpnetsecurity.com/2026/09/04 /google-chrome-zero-day-cve-2026-85046/) - 2026-09-04 - corroborated by [The Hacker News](https://thehackernews.com/2026/09/google-releases-chro me-update-to-patch.html) and [CISA KEV catalog](https://www.cisa.gov/known-exploited-vulnerabilitie s-catalog)

ACTIVELY EXPLOITED

Working root-privilege-escalation exploit published for a Linux kernel SCTP use-after-free

WHAT HAPPENED

Public proof-of-concept exploit code landed for a use-after-free in the Linux kernel's SCTP stack (triggered when a Stale Cookie ERROR rolls an association back from COOKIE_ECHOED to COOKIE_WAIT while data is queued). It's a companion bug to the recently-disclosed "SCTPhantom" flaw and was initially under-rated as a denial-of-service issue before the PoC showed it drives full local root.

AFFECTED

Distribution kernels that have not picked up the SCTP stream-scheduler fix issued in early August 2026 (Debian, Ubuntu, RHEL/Rocky and derivatives are all in scope until patched - check your distro's kernel changelog rather than trusting the version string alone, since backports don't always bump the version number).

EXPLOITATION

Public PoC/exploit released - reported by security research outlet securityonline.info, exploit code published to GitHub.

FIX

Update to a kernel build that includes the SCTP outqueue-purge fix for stale-cookie handling (shipped alongside/after the SCTPhantom fixes in early August 2026). Where SCTP isn't required, blacklist the `sctp` kernel module as a stopgap.

CHECK IF YOU'RE EXPOSED

`lsmod | grep sctp` to see if the module is loaded; if you can't confirm your kernel package includes the post-August-6 SCTP fix, treat the host as exposed and prioritize the module blacklist until patched.

SOURCE

[securityonline.info - CVE-2026-52924 PoC Exploit Disclosed: 9.8 CVSS Linux Root Privilege Escalation](https://securityonline.info/linux-cve-2026-52924 -poc/) - 2026-09-05 - background via [The Hacker News - 18-Year-Old Linux SCTP Flaw](https://thehackernews.com/2026/08/18-year-old-linux-sc tp-flaw-could-let.html)

Note: the seven CISA KEV additions from 2026-09-02 (Sangoma Switchvox, Kestra OSS, LiteLLM, JFrog Artifactory, SonicWall SMA1000 x2, Kludex Starlette) and the PaperCut/JFrog/SonicWall/GeoServer/ownCloud/cPanel/VMware/Fi re Ant items from prior briefs remain live and unpatched-fleet risk, but nothing material changed on them beyond the PaperCut campaign above in this 48-hour window.