



THREAT ADVISORY

TLP: CLEAR

AI-GENERATED ZERO-DAY EXPLOIT CHAINS

What Anthropic's October 2026 disclosure means for your organization, which fixes are available, and what to do while the Linux kernel gap remains open.

BOTTOM LINE

FOUR OF FIVE CHAINS ARE PATCHED. LINUX IS THE OPEN GAP.

On October 27, 2026, Anthropic's Frontier Red Team published five attack chains that an unreleased internal AI model found and turned into working exploits: Chrome, Safari, Android, Windows and Linux. Four are fixed by their vendors. The Linux zero-click remote root chain (CVE-2026-98432) is fixed upstream, but as of October 30 there is no fixed kernel from Ubuntu or Red Hat.

BROWSERS & APPLE

Patched. Chrome 156 (October 20) and Apple's fix are out. The work is confirming deployment, including other Chromium-based browsers.

WINDOWS

Patched since April 14, 2026. The impact is loss of availability, not code execution.

LINUX

Fixed upstream, not yet in Ubuntu or RHEL kernels. Red Hat reports no mitigation that meets its standards.

WHAT'S ACTUALLY NEW

None of the sources we reviewed reports exploitation in the wild, and no exploit code has been published. What is new is the capability: Anthropic says the model found the flaws and chained them into working exploits after initial prompting. That claim is self-reported and can't be independently checked, but it suggests the time between a fix and a working exploit may keep shrinking.

VULNERABILITY DETAILS

Only two of the five chains have a single named CVE. Chrome covers 62 CVEs, and Safari and Android have no public identifier in the sources we reviewed.

Platform	Identifier	What the chain does	Severity	Fix status
Chrome	62 CVEs (13 sandbox escapes, 21 renderer compromises)	Four chained bugs (V8 heap corruption, V8 sandbox escape, CacheStorage race, FedCM use-after-free) run code outside the browser sandbox	Critical or high	Fixed in Chrome 156, stable October 20
Safari	None found	Use-after-free in JavaScriptCore plus Gigacage and sandbox-IPC bypasses turn off the same-origin policy; data theft, no code execution	Not rated	Fixed; Apple advisory 127594; iOS and iPadOS 26.5.2
Android	None found	Chains three flaws to pull photos and data off a locked Pixel 9 over USB	Not rated	Anthropic says Google fixed it; no public record found
Windows	CVE-2026-33096	Out-of-bounds read; a few packets crash and restart a server that answers HTTP/3, repeatedly	CVSS 7.5, Microsoft "Important"	Fixed in April 14, 2026 Patch Tuesday

Platform	Identifier	What the chain does	Severity	Fix status
Linux	CVE-2026-98432	Race-condition use-after-free in the IPv4 TCP handshake; the proof of concept reaches root on servers with a multipath TCP (MPTCP) listener	9.8 per kernel CVE team; vendors 5.9 to 8.1	Fixed upstream; most distributions not yet

The Linux bug was introduced in kernel 4.4, and the upstream fix landed October 5. IPv6 is not affected by this race. Fixed upstream versions: 5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.56, 7.2.10 and 7.3.

ATTACK REQUIREMENTS

None of the five chains needs credentials. The practical gates are whether a user visits a hostile page, whether a server is reachable and, for Linux, whether it exposes an MPTCP listener.

Chain	Attacker position	User action	What must be true	Notes
Chrome	Remote, via a web page	One click or page load	Unpatched Chrome	Code runs as the user, outside the sandbox
Safari	Remote, via a web page	Visit the page	Unpatched Safari and Apple OS	No code execution, so endpoint tools have little to detect. Reads cookies, history and sessions
Android	Physical	None	Stolen locked phone, USB connection	Tested on Pixel 9. Not a remote risk
Windows	Network	None	Server answers HTTP/3 using the native Windows implementation	Repeat requests keep the server down. No code execution or data theft
Linux	Network	None	Reachable server on a vulnerable kernel; MPTCP listener in the proof of concept	Failed attempts don't crash the host, so attackers can retry. The proof of concept reached a root shell in about 53 minutes

TWO POINTS ABOUT THE LINUX CHAIN

- **MPTCP exposure may be wider than expected.** Go programs have requested MPTCP by default for listening sockets since Go 1.24, per the Go Security Team, so a server can have an MPTCP listener without anyone choosing it.
- **The bug is not MPTCP-specific.** The CVE record and kernel fix describe an IPv4 TCP flaw and never mention MPTCP. Whether servers without MPTCP listeners can be taken over to root has not been established.

The severity scores differ. The kernel CVE team rates attack complexity low (9.8) because both sides of the race are attacker-induced. SUSE and Amazon score it 8.1, rating complexity high because the race is hard to win, and Red Hat's draft score is 5.9, treating denial of service as the practical worst case. The kernel CVE team notes the bug can also leak kernel memory over the network or crash the kernel, and Anthropic's proof of concept shows root is achievable in the lab.

POTENTIAL IMPACT

Chain	Impact if exploited	Who is exposed
Linux	Root on the server: data theft, persistence, ransomware staging, pivot into the network	Internet-facing Linux servers on unpatched kernels

Chain	Impact if exploited	Who is exposed
Chrome	Code execution as the signed-in user: credential and session-token theft, foothold for lateral movement	Endpoints on Chrome below 156, and other Chromium-based browsers until their updates land
Safari	Reading other sites' data in the user's session, including webmail, banking and cloud consoles	Apple devices not yet updated
Windows	Repeated crash and restart of servers that answer HTTP/3; loss of access for all users	Internet-facing Windows servers without the April 2026 updates
Android	Photos and personal data from a stolen locked phone	Lost or stolen Pixel devices

OUR VIEW BY SECTOR

- **Healthcare:** Linux application and database servers holding PHI make the Linux chain the main concern; a root compromise would require a breach assessment.
- **Financial services:** Safari session theft and Chrome token theft target client portals and banking sessions; Linux hosting is the second concern.
- **Higher education:** large, mixed internet-facing estates and unmanaged personal browsers widen exposure to all three network and browser chains.
- **Technology and energy:** Linux and cloud workloads dominate, so the Linux chain matters most.

CONFIRMED VERSUS UNVERIFIED

The patches and credits are verifiable with vendors. How autonomous the model was, and how two of the CVEs map to Anthropic's descriptions, are not.

Claim	Status	Basis
Chrome 156 fixes the reported bugs	Confirmed	Chrome release notes credit Anthropic researchers, assisted by Claude, for several fixes
Apple fixed the Safari chain	Confirmed	Apple credits Anthropic researchers with Claude; fix in iOS and iPadOS 26.5.2
Windows CVE-2026-33096 exists, 7.5, patched April 2026	Confirmed	NVD and Microsoft record
Linux CVE-2026-98432 exists, 9.8 from the kernel CVE team	Confirmed	CVE record; kernel fix credits an Anthropic researcher
No exploitation in the wild	Not reported	No vendor or CERT reports it; not in the CISA KEV catalog as of October 30
Model built the chains with little human involvement	Unverified	Self-reported; no breakdown of human involvement at each step
Windows bug is the QUIC flaw Anthropic describes	Unverified	Anthropic says kernel QUIC code; the public record says HTTP.sys
Linux root exploit uses CVE-2026-98432 via MPTCP	Unverified link	The record and fix never mention MPTCP
Android chain is fixed	Unverified	Anthropic says Google fixed it; no public record found

Anthropic's disclosure policy gives vendors 90 days to patch before details are discussed further, but the Linux fix commit is public and anyone can study it. Treat that as a reason to move quickly on Linux kernels, not as a confirmed threat.

LINUX DISTRIBUTION STATUS

Checked against vendor trackers as reported October 30. Status changes daily; check your vendor's advisory before acting.

Distribution	Status	Fixed package
Ubuntu 22.04, 24.04, 26.04, 26.10	In progress	None released. Watch for linux 6.8.0-149.149 (24.04) and 5.15.0-203.213 (22.04), generic kernels
Ubuntu 16.04, 18.04, 20.04	Vulnerable	None released
RHEL 8, 9, 10 and OpenShift 4	Not fixed	None released, no date announced
RHEL 7	Not affected	Not needed
Debian 13 (trixie) and 12 (bookworm)	Fixed	trixie linux 6.12.113-1 (DSA-6568-1); bookworm per DLA-4841-1 and DLA-4850-1
Oracle Linux 7 to 10 (UEK)	Fixed	ELSA-2026-500397, -500398, -500399
Amazon Linux 2023, kernel6.18 and kernel6.12	Fixed	ALAS2023-2026-3251 and ALAS2023-2026-3335
Amazon Linux 2023 default kernel; Amazon Linux 2	Pending	None released
SLES 16.0, openSUSE Leap 16.0, SL Micro 6.2	Fixed	kernel-default 6.12.0-160000.40.1 or later
SLES 15 SP4 to SP6 LTSS, SLE Micro 5.3 to 5.5	Fixed	Per SUSE's CVE page for each release
SLES 15 SP7	In progress	None released

On mitigations: Red Hat says no available mitigation meets its standards. Setting `GODEBUG=multiplaytcp=0` disables MPTCP in Go programs, but the Go Security Team calls it fragile, since one exposed MPTCP listener still leaves a system open and the bug is not MPTCP-specific. Disabling MPTCP system-wide with `sysctl` stops new MPTCP sockets but does not close listeners that are already open. Some practitioners suggest dropping inbound IPv4 packets that carry IP options at the network edge, since the trigger relies on them; no vendor has confirmed this as a mitigation, so treat it as defense in depth and test before deploying.

RECOMMENDED ACTIONS

- ☐ **Update Chrome to 156.0.8078.73 or later** on Windows, macOS and Linux, and confirm other Chromium-based browsers (such as Edge and Brave) have shipped their corresponding fixes.
- ☐ **Update iPhones and iPads to iOS and iPadOS 26.5.2 or later**, and apply Apple's corresponding macOS and Safari updates listed in advisory 127594.
- ☐ **Confirm the April 14, 2026 Windows updates** on internet-facing servers that answer HTTP/3.
- ☐ **Inventory Linux servers** by distribution, kernel flavor, running kernel version and internet exposure. Identify MPTCP listeners (for example with `ss -Mlnp`), including Go-based services that may open them by default.

- ☐ **Apply fixed kernels where they exist, then reboot.** Debian, Oracle UEK, most SUSE releases and some Amazon Linux packages have fixes. A new kernel does nothing until the server boots into it, so confirm the running version with `uname -r`. Watch Ubuntu and Red Hat advisories for fixed releases.
- ☐ **Until a fixed kernel is available, reduce exposure.** Limit who can reach internet-facing listeners, consider placing exposed services behind a gateway, and confirm `net.ipv4.tcp_migrate_req` is 0 (the default), which closes a secondary trigger path. These reduce risk but are not vendor-validated mitigations.
- ☐ **Keep managed mobile devices on the current security patch level.**
- ☐ **Revisit patch timelines.** If working exploits can appear sooner after a fix, timelines for browsers, Apple devices and internet-facing servers may need to tighten. This ties directly to audited controls such as NIST SP 800-53 SI-2 and PCI DSS 6.3.

HOW LEGION CYBERWORKS CAN HELP

VALIDATE YOUR EXPOSURE

Continuous pentesting with NodeZero shows which systems an attacker can actually reach and exploit, and verifies fixes.

PATCH AND VERIFY

Managed endpoint and Microsoft 365 security keeps browsers, devices and servers on current versions with reporting to prove it.

WATCH AROUND THE CLOCK

24/7 managed detection and response investigates suspicious activity on endpoints and servers.

LEAD THE RESPONSE

Our Fractional CISOs help you decide on interim risk measures and communicate them to leadership.

NOT SURE IF YOU'RE EXPOSED?

Talk to our team at legioncyber.com/contact.

SOURCES

- Anthropic: [Discovering and exploiting vulnerabilities in critical, real-world software with Claude](#) (October 27, 2026)
- The Hacker News: [Anthropic's Unreleased AI Model Chains Flaws Into Working Chrome, Safari, Windows and Linux Exploits](#) (October 28, 2026)
- The Hacker News: [Linux Kernel TCP Flaw With 9.8 CVSS Score Affects Ubuntu, Red Hat and Other Distributions](#) (October 29, updated October 30, 2026)
- Cyber Security News: [Claude AI Builds One-Click Chrome and 0-Click Linux Exploit Chains](#) (October 28, 2026)
- Vendor trackers for CVE-2026-98432: [Ubuntu](#), [Red Hat](#), [Debian](#), [SUSE](#), [Amazon Linux](#), [Oracle Linux](#)
- NVD: [CVE-2026-33096](#); Chrome Releases: [Stable Channel Update for Desktop](#) (October 20, 2026)

TLP:CLEAR. This advisory reflects publicly available information as of October 30, 2026, and is provided for general informational purposes only. It is not legal advice and does not guarantee the security of any system. Vulnerability and patch status change frequently; confirm current status with each vendor before acting. © 2026 Legion Cyberworks LLC. legioncyber.com