INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

CVE-2026-3909: Google Skia Out-of-Bounds Write, Active Exploitation via Crafted HTML

CVE VULNERABILITY | HIGH | CVSS 8.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0016
Type	CVE Vulnerability
CVE ID	CVE-2026-3909
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.3306 (97th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-03-27)
Affected Products	Google Skia (affects Google Chrome, ChromeOS, Android, Flutter, and potentially other Skia-dependent products)
Published	2026-03-13

Executive Summary

A high-severity out-of-bounds write vulnerability in Google Skia (CVE-2026-3909, CVSS 8.8) is actively exploited in the wild and listed in CISA's Known Exploited Vulnerabilities catalog. Attackers can trigger the flaw by directing users to a crafted web page, requiring no authentication and no user action beyond visiting the page. Any organization running Google Chrome, ChromeOS, Android devices, or Flutter-based applications is at risk of device compromise through routine web browsing.

Technical Analysis

CVE-2026-3909 is an out-of-bounds write (CWE-787) in Google Skia, the open-source 2D graphics rendering library embedded in Chrome, ChromeOS, Android, and Flutter. The attack vector is remote and requires low complexity: a threat actor hosts a crafted HTML page that triggers malformed rendering instructions, causing Skia to write beyond allocated memory boundaries. Successful exploitation commonly leads to arbitrary code execution or memory corruption in the context of the browser renderer process. MITRE maps this to T1203 (Exploitation for Client Execution) and T1189 (Drive-by Compromise). EPSS score is 0.33 at the 96.8th percentile, indicating very high relative exploitation probability compared to all scored CVEs. CISA KEV due date for federal agencies is 2026-03-27. Patch status should be confirmed against the Google Chrome Releases blog (https://chromereleases.googleblog.com/) and NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-3909). No specific affected version range is confirmed in the provided

data; consult the NVD record and Google security advisory for version-specific guidance.

Action Checklist

1. Step 1, Patch immediately: Update Google Chrome to the latest stable release. Apply available ChromeOS and Android security updates. Confirm patch versions against the Google Chrome Releases blog and NVD CVE-2026-3909 record before closing the action.
2. Step 2, Inventory exposure: Identify all Chrome, ChromeOS, Android, and Flutter deployments across managed endpoints, mobile devices, and embedded systems. Include unmanaged BYOD devices with access to corporate resources.
3. Step 3, Detect exploitation attempts: Query endpoint detection logs and browser telemetry for renderer process crashes, unusual child process spawning from Chrome, or memory access violations associated with Skia rendering. Review proxy and DNS logs for drive-by delivery patterns (high-redirect chains, newly registered domains serving HTML).
4. Step 4, Enforce browser update policy: Verify auto-update is enabled and enforced via MDM or Group Policy for all managed Chrome and ChromeOS instances. Identify any systems with update deferrals or exceptions and escalate for immediate manual patching.
5. Step 5, Notify affected stakeholders: Inform IT, SOC, and device management teams of CISA KEV status and the 2026-03-27 federal remediation deadline. If your organization follows CISA BOD 22-01 or equivalent patch SLA policy, open a formal tracking ticket with the KEV due date.
6. Step 6, Review scope beyond Chrome: Assess whether any internally developed or third-party applications use Flutter or embed Skia directly. Those products require separate vendor patch confirmation and may not be covered by Chrome update cadence.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to Chief Information Security Officer (CISO) and external IR firm engagement if: (1) exploitation is confirmed on any endpoint (renderer crash with out-of-bounds memory signatures), (2) BYOD device inventory shows >10% unpatched coverage, or (3) internally developed critical applications cannot be patched within 72 hours due to vendor delays.
Recovery Notes	Post-containment, verify patch deployment to 100% of inventory via automated compliance scanning (Tenable Nessus, Qualys, Rapid7). For any system where exploitation is suspected (process crashes, unusual child processes), perform full disk forensic imaging per chain-of-custody protocol and analyze for persistence mechanisms (browser extensions, kernel modules, scheduled tasks). Review Chrome sync logs and browsing history for malicious redirect chains to identify attacker-controlled infrastructure for threat intelligence handoff.

Forensic Artifacts	Windows Event ID 4688 (Process Creation) with chrome.exe and child processes, 30 days pre-incident to incident closure | C:\Users*\AppData\Local\Google\Chrome\User Data\Crashpad\reports (Chrome crash minidumps with Skia rendering stack traces) | /var/log/syslog and dmesg logs for segmentation fault signatures matching Chrome PID on Linux systems | Proxy/firewall access logs with full HTTP headers (User-Agent, Referer, Set-Cookie) showing redirect chains and domain registration age | Chrome History database (C:\Users*\AppData\Local\Google\Chrome\User Data\Default\History) and Android browser cache (/data/data/com.android.chrome/app_chrome/) for malicious landing pages

Per-Action IR Details

Step 1 — Patch immediately: Update Google Chrome to the latest stable release. Apply available ChromeOS and Android security updates. Confirm patch versions against the Google Chrome Releases blog and NVD CVE-2026-3909 record before closing the action.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3.3 (Eradication); NIST 800-61r3 §4.1 (Preparation — patch management baseline)

Controls: NIST SI-2 (Flaw Remediation), CIS 3.10 (Address Unauthorized Software)

Compensating: If auto-update is disabled, use Chrome's --enable-automatic-updates flag via GPO/MDM or manually verify version via chrome://version comparing against NVD database. For ChromeOS, verify via Settings > About > Check for updates. For Android, confirm via Settings > Apps > Google Play > Chrome > Update available or adb shell dumpsys package com.android.chrome | grep versionName on enrolled devices.

Evidence: Capture pre-patch Chrome version strings (chrome://version), registry hive HKLM\Software\Google\Chrome for update policy state, and Group Policy audit logs (Event ID 4719) showing policy application before patching. For Android, capture adb logcat output for crash signatures matching 'Skia' or 'renderer process'.

Step 2 — Inventory exposure: Identify all Chrome, ChromeOS, Android, and Flutter deployments across managed endpoints, mobile devices, and embedded systems. Include unmanaged BYOD devices with access to corporate resources.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — detection tools); NIST 800-53 CM-2 (Baseline Configuration)

Controls: CIS 1.1 (Inventory and Control Hardware Assets), CIS 2.1 (Inventory and Control Software Assets), NIST IA-4 (Identifier Management)

Compensating: Query DHCP/DNS logs for Chrome user-agent strings (case-insensitive grep 'Chrome/' across proxy logs). For endpoints: use osquery or auditd to enumerate /opt/google/chrome or C:\Program Files\Google\Chrome presence and version. For Android: cross-reference MDM enrollment roster against device OS type; query corporate VPN logs for Android user-agent patterns. For Flutter apps, query application inventory spreadsheet or run strings/egrep on app binaries for 'flutter.io' or Skia library signatures.

Evidence: Collect baseline CMDB/asset management export (include Chrome version, OS, patch level). Capture DHCP lease logs with user-agent associations. For forensic readiness: preserve MDM enrollment snapshots and app distribution catalogs dated before patch release to establish pre-incident inventory chain.

Step 3 — Detect exploitation attempts: Query endpoint detection logs and browser telemetry for renderer process crashes, unusual child process spawning from Chrome, or memory access violations associated with Skia rendering. Review proxy and DNS logs for drive-by delivery patterns (high-redirect chains, newly registered domains serving HTML).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Analysis — event correlation); NIST 800-53 SI-4 (Information System Monitoring)

Controls: CIS 8.2 (Enable Detailed Logging), CIS 8.5 (Ensure Detailed Logging for Web Applications), NIST DE.CM-1 (Detection processes and tools)

Compensating: Without SIEM: grep Windows Event ID 4688 (Process Creation) for chrome.exe with child process abnormalities (e.g., cmd.exe, powershell.exe spawned from chrome.exe or conhost.exe as child of chrome). Check C:\Windows\System32\winevt\Logs\Application.log and C:\Windows\System32\winevt\Logs\System.log for crash dump references. For Linux: parse /var/log/syslog for segmentation fault patterns matching Chrome PID. Query proxy access logs (Squid, pfSense, etc.) for redirect chains (>5 hops in single session) or domains registered <7 days before incident. Use tcpdump -r capture.pcap 'tcp.flags.syn==1 && ip.dst != internal_range' to identify outbound connections from Chrome process.

Evidence: Capture process memory dumps from Chrome renderer processes showing crashed state (use ProcDump -mp chrome.exe or gcore on Linux). Preserve full proxy access logs 30 days pre-incident with headers (User-Agent, Referer, response codes). Archive Windows ETW trace (netsh trace start capture=yes) or tcpdump capture spanning exploitation window. Extract Chrome crash minidumps from C:\Users*\AppData\Local\Google\Chrome\User Data\Crashpad\reports or ~/.config/google-chrome/Crash Reports/.

Step 4 — Enforce browser update policy: Verify auto-update is enabled and enforced via MDM or Group Policy for all managed Chrome and ChromeOS instances. Identify any systems with update deferrals or exceptions and escalate for immediate manual patching.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3.1 (Eradication — identifying systems); NIST 800-53 CM-5 (Access Restrictions for Change)

Controls: NIST SI-2 (Flaw Remediation), CIS 2.4 (Ensure Software is Up to Date), NIST CM-3 (Change Control)

Compensating: For Group Policy: gpresult /h report.html on each endpoint, search for 'Google\Update\UpdateDefault\' registry values (default 1 = auto-update enabled; if value is 0 or absent, escalate). For MDM-managed devices: export MDM compliance report filtering on Chrome version field; any device >1 version behind current release fails compliance. For non-managed endpoints: use Jamf, Intune, or MobileIron API to query device OS and Chrome version; flag BYOD devices for BYOD policy violation. Use auditd rule: -w /etc/cron.* -p wa -k update_policy_change to detect disable attempts.

Evidence: Export pre-enforcement Group Policy audit logs (Event ID 4719 for policy changes). Capture MDM configuration export showing Chrome update policy state per device group. Preserve registry export from HKLM\Software\Policies\Google\Chrome showing UpdateDefault setting. For BYOD: document device OS type and last-seen Chrome version from MDM portal with timestamp.

Step 5 — Notify affected stakeholders: Inform IT, SOC, and device management teams of CISA KEV status and the 2026-03-27 federal remediation deadline. If your organization follows CISA BOD 22-01 or equivalent patch SLA policy, open a formal tracking ticket with the KEV due date.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Preparation — communication); NIST 800-53 IR-1 (Incident Response Policy)

Controls: CIS 17.1 (Designate Individuals to Fulfill Communications Plan Roles), NIST IR-2 (Incident Response Training)

Compensating: No tool required. Create plaintext ticket in tracking system (Jira, GitHub Issues, ServiceNow, or email) with: CVE-2026-3909, CVSS 8.8, CISA KEV date, 2026-03-27 SLA deadline, list of affected product families (Chrome, ChromeOS, Android, Flutter apps). Include link to CISA NVD page. For organizations subject to federal contract terms (FAR, DFARS, or equivalent): annotate ticket with 'Federal Remediation Deadline' and route to Compliance or Contracting office for acknowledgment.

Evidence: Preserve ticket creation timestamp and stakeholder acknowledgment log (email read receipts, Slack reaction timestamps, or ticket assignment confirmation). Document in incident response log per NIST 800-61r3 §3.4.2.

Step 6 — Review scope beyond Chrome: Assess whether any internally developed or third-party applications use Flutter or embed Skia directly. Those products require separate vendor patch confirmation and may not be covered by Chrome update cadence.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — detection and analysis tools); NIST 800-53 CM-2 (Baseline Configuration)

Controls: CIS 2.1 (Inventory and Control Software Assets), NIST SA-3 (System Development Life Cycle)

Compensating: Scan application binaries for Skia library signatures: strings /path/to/app | grep -i 'skia\|flutter\|//third_party/skia' or objdump -t /path/to/app | grep skia. Query build manifests (package.json, pubspec.yaml, gradle.build, pom.xml, CMakeLists.txt) for direct Flutter or Skia dependencies. Request vendor advisory/patch status via email and document responses in tracking system. For internal apps: contact development team, provide CVE details, request patched Skia library version and release date. Create separate incident ticket per third-party product requiring patch coordination.

Evidence: Preserve application inventory spreadsheet with library dependency audit (Skia version, Flutter version, build date). Capture vendor patch advisory emails or ticket responses with promised patch dates. Archive application binary hashes (SHA-256) pre- and post-patch for integrity verification. Document source code repository commits showing Skia library update with timestamp.

Detection Guidance

No specific IOCs (IPs, domains, hashes) are confirmed in the available source data for CVE-2026-3909. Detection should focus on behavioral and telemetry signals. On endpoints running Chrome: monitor for renderer process (chrome.exe --type=renderer) spawning unexpected child processes or making network connections. Watch for Chrome crash reports (crashpad_handler activity) clustered around the same time period across multiple hosts, which may indicate in-the-wild probing. At the network perimeter: flag HTTP/HTTPS sessions where the browser receives a large, complex HTML or SVG payload from a newly registered or low-reputation domain, followed immediately by unusual process activity on the client. In EDR telemetry: alert on memory access violations or heap corruption signals originating from the Skia rendering pipeline. MITRE T1189 (Drive-by Compromise) detection logic, proxy logs showing short session durations with immediate redirect chains ending at content-heavy pages, is applicable here. Prioritize detection coverage on unpatched endpoints until patch verification is complete.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1189** — Drive-by Compromise

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10**

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1189	Drive-by Compromise	Initial-Access

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
(consolidated)	https://securityboulevard.com/2026/03/cve-2026-3342-critical-out-of...	T3
CVE-2026-3909 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3909	T1
CVE-2026-3909 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-3909	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_...	T1
Google Security Advisory	https://chromereleases.googleblog.com/	T1

Generated 2026-03-29 18:33 UTC by TJS Security Command Center