INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 19:29 UTC

Google Chromium V8 Out-of-Bounds Read/Write Zero-Day, Active Exploitation (CVE-2026-11645)

CVE VULNERABILITY | HIGH | CVSS 8.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0276
Type	CVE Vulnerability
CVE ID	CVE-2026-11645
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0008 (24th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-06-23)
Affected Products	Google Chromium V8 JavaScript Engine (affects Google Chrome, Microsoft Edge, Opera, and other Chromium-based browsers)
Published	2026-06-09
Discovery Source	Cisa Kev

Executive Summary

A high-severity zero-day vulnerability in the V8 JavaScript engine affects all Chromium-based browsers, including Google Chrome, Microsoft Edge, and Opera. Attackers can compromise any user's device simply by directing them to a malicious webpage, requiring no additional user interaction beyond visiting the site. CISA has confirmed active exploitation in the wild, making this an immediate patching priority for all organizations whose employees use Chromium-based browsers.

Technical Analysis

CVE-2026-11645 is an out-of-bounds read/write vulnerability (CWE-787, CWE-125) in the Google Chromium V8 JavaScript engine. Attack vector is network-based with low attack complexity and no required privileges; user interaction is limited to visiting a crafted HTML page (MITRE T1189, Drive-by Compromise, T1203, Exploitation for Client Execution). Successful exploitation enables arbitrary code execution within the browser sandbox. CVSS base score is 8.8 (High). CISA added this to the Known Exploited Vulnerabilities catalog with a federal remediation due date of 2026-06-23, confirming in-the-wild exploitation. Affected products span all Chromium-based browsers. Google has issued a patch; organizations should verify deployed browser versions against Google's advisory. Sources: CISA KEV (T1), NVD (T1), Microsoft Security Response Center (T1).

Action Checklist

1. Step 1: Containment. Immediately verify that Chrome auto-update is enabled across all managed endpoints. For environments where auto-update is disabled or delayed, push the patched Chrome version via your endpoint management platform (Intune, SCCM, Jamf) before end of business today. Apply the same urgency to Microsoft Edge via the Microsoft Security Response Center official advisory. Block access from unmanaged or unpatched Chromium-based browsers to corporate resources until version compliance is confirmed. Reference: NIST AC-17 (Remote Access), CIS 4.6 (Securely Manage Enterprise Assets and Software).
2. Step 2: Detection. Query endpoint management and EDR telemetry for browser version numbers across all assets; flag any Chrome or Edge installations below the patched version. In your SIEM, search for renderer process crashes or unusual child process spawning from browser processes, which can indicate sandbox escape attempts. Review proxy and web gateway logs for repeated visits to low-reputation or newly registered domains, consistent with drive-by delivery (T1189). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Apply the vendor-issued patch to all Chromium-based browsers: update Chrome to the version specified in Google's release advisory, update Edge to the version specified in the Microsoft Security Response Center advisory, and update any other Chromium-based browsers (Opera, Brave, Vivaldi) to their respective patched releases. Confirm no shadow IT browser installations exist by cross-referencing CIS 1.1 (Enterprise Asset Inventory) and CIS 2.1 (Software Inventory). Reference: NIST SI-2 (Software Updates), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, re-query endpoint management to confirm 100% version compliance. Run a browser process integrity check via EDR to confirm no persistence artifacts remain in browser profile directories or extensions. Monitor web proxy logs for 48 hours post-patch for any continued anomalous outbound connections from browser processes. Validate that browser auto-update policies are enforced and functioning. Reference: NIST AU-6, CIS 8.2.
5. Step 5: Post-Incident. Review browser update deferral policies; this zero-day demonstrates that any patch delay window is an active exposure window for browser CVEs. Assess whether your software inventory (CIS 2.1) captures all Chromium-based browsers, not only Chrome and Edge. Evaluate web content filtering and DNS-based threat blocking to reduce drive-by exposure surface. Consider whether users require all Chromium-based browsers or whether the approved list can be narrowed. Reference: CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 4.6, NIST CM-7 (Least Functionality).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal counsel immediately if any host is confirmed to have executed post-sandbox-escape code from CVE-2026-11645 exploitation (evidenced by unexpected child processes from chrome.exe/msedge.exe, malicious extensions, or unexplained outbound C2 connections from browser processes), as this constitutes a confirmed device compromise with potential access to user credentials, session tokens, and any data accessible within the browser profile, triggering breach notification assessment under applicable data protection regulations (GDPR, HIPAA, state privacy laws) if PII or PHI was accessible.
Recovery Notes	After confirming 100% patch compliance via endpoint management version query, perform a targeted review of browser extension inventories on all hosts that were running unpatched Chromium versions during the active exploitation window, as post-sandbox-escape persistence via malicious extensions can survive a browser update if the extension directory is not cleared. Monitor outbound network connections initiated by chrome.exe and msedge.exe processes for a minimum of 48 hours post-patch using proxy logs or host-based firewall audit logs, flagging any connections to domains or IPs not present in pre-incident baseline traffic. Validate that Google Update and Microsoft EdgeUpdate services are running and unmodified on all endpoints, as a sophisticated attacker may have tampered with the update mechanism to prevent future patching.
Forensic Artifacts	Crashpad renderer crash dumps at '%LOCALAPPDATA%\Google\Chrome\User Data\Crashpad\reports\' and '%LOCALAPPDATA%\Microsoft\Edge\User Data\Crashpad\reports\' — V8 OOB read/write exploitation frequently generates renderer crash reports immediately before or during a successful exploit, and these .dmp files contain memory state at time of crash that can confirm exploitation of CVE-2026-11645. | Browser extension directories at '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\' and the Edge equivalent — post-sandbox-escape persistence from this class of V8 exploit commonly manifests as a silently installed or modified extension; hash all extension manifest.json and background script files and compare against the Chrome Web Store or known-good baselines. | Sysmon Event ID 1 (Process Create) and Event ID 10 (Process Access) logs filtered on chrome.exe and msedge.exe as parent or source processes — unexpected child processes (cmd.exe, powershell.exe, wscript.exe) or cross-process memory access to lsass.exe originating from browser renderer processes are direct indicators of a successful sandbox escape following CVE-2026-11645 exploitation. | Web proxy and gateway access logs filtered on the user-agent strings of affected Chromium versions (pre-patch Chrome and Edge builds) for the 72-hour window preceding detection — these logs identify which endpoints contacted potential drive-by delivery infrastructure consistent with T1189, and the destination domains/IPs become primary IOCs for the investigation. | Windows registry export of 'HKLM:\Software\Google\Chrome\BLBeacon' (version key) and 'HKCU:\Software\Google\Chrome\BLBeacon' (user-installed copies) timestamped before patching — this documents the exact pre-patch version present on each host and establishes which endpoints were running vulnerable Chromium builds during the active exploitation window confirmed by CISA.

Per-Action IR Details

Step 1: Containment — Immediately verify that Chrome auto-update is enabled across all managed endpoints. For environments where auto-update is disabled or delayed, push the patched Chrome version via your endpoint management platform (Intune, SCCM, Jamf) before end of business today. Apply the same urgency to Microsoft Edge via Microsoft Update Catalog (per the Microsoft Security Advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11645). Block access from unmanaged or unpatched Chromium-based browsers to corporate resources until version compliance is confirmed.

Reference: NIST AC-17 (Remote Access), CIS 4.6 (Securely Manage Enterprise Assets and Software).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without Intune/SCCM/Jamf: run 'wmic product where name like "Google Chrome%" get version' or PowerShell 'Get-ItemProperty HKLM:\Software\Google\Chrome\BLBeacon -Name version' across all Windows hosts via PsExec batch script to inventory unpatched Chrome instances. For Edge: query registry at 'HKLM:\SOFTWARE\Microsoft\EdgeUpdate\Clients\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}' for the pv value. Block unpatched hosts at the network firewall or NAC by placing them in a quarantine VLAN until version compliance is confirmed — no EDR required.

Evidence: Before pushing patches, capture a snapshot of installed browser versions from each endpoint (registry exports from HKLM:\Software\Google\Chrome\BLBeacon and HKLM:\SOFTWARE\Microsoft\EdgeUpdate\Clients), along with proxy/web gateway logs showing which endpoints contacted external web destinations in the 72 hours prior to detection — these establish baseline exposure for any host that may have visited a CVE-2026-11645 delivery page before containment. Preserve endpoint management console reports (Intune device compliance export, SCCM hardware inventory) timestamped before patching begins to document the pre-patch version state.

Step 2: Detection — Query endpoint management and EDR telemetry for browser version numbers across all assets; flag any Chrome or Edge installations below the patched version. In your SIEM, search for renderer process crashes or unusual child process spawning from browser processes, which can indicate sandbox escape attempts. Review proxy and web gateway logs for repeated visits to low-reputation or newly registered domains, consistent with drive-by delivery (T1189). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR: deploy Sysmon with the SwiftOnSecurity config and query Windows Event Log for Event ID 1 (Process Create) where ParentImage matches chrome.exe or msedge.exe and Image is NOT a known browser helper (flag cmd.exe, powershell.exe, wscript.exe, or mshta.exe as children — these indicate a sandbox escape from a V8 exploit). For renderer crashes specific to V8 OOB exploitation, check '%LOCALAPPDATA%\Google\Chrome\User Data\Crashpad\reports' and '%LOCALAPPDATA%\Microsoft\Edge\User Data\Crashpad\reports' for .dmp files timestamped during the exposure window. Parse proxy logs with grep/PowerShell for domains registered within the last 30 days (cross-reference with a free feed such as WhoisXML or CIRCL passive DNS) that were accessed by browser processes.

Evidence: Capture Crashpad crash dumps from '%LOCALAPPDATA%\Google\Chrome\User Data\Crashpad\reports\' and the equivalent Edge path before any browser restart or update overwrites them — a V8 OOB read/write exploit will frequently generate renderer process crashes immediately before or during a successful exploitation attempt. Collect Sysmon Event ID 1 and Event ID 10 (ProcessAccess) logs showing chrome.exe or msedge.exe renderer processes attempting to access lsass.exe or spawning unexpected child processes, which are indicators of post-sandbox-escape lateral movement. Export proxy/web gateway logs for the exposure window filtered on the user-agent strings of the affected Chromium versions to identify which endpoints visited potential delivery infrastructure.

Step 3: Eradication — Apply the vendor-issued patch to all Chromium-based browsers: update Chrome to the version specified in Google's release advisory, update Edge to the version specified in the Microsoft Security Advisory (msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11645), and update any other Chromium-based browsers (Opera, Brave, Vivaldi) to their respective patched releases. Confirm no shadow IT browser installations exist by cross-referencing CIS 1.1 (Enterprise Asset Inventory) and CIS 2.1 (Software Inventory). Reference: NIST SI-2 (no mapped control in provided knowledge base for SI-2 — see NIST SP

800-53 Rev. 5 directly), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: For shadow IT browser discovery without enterprise tooling: run 'Get-ChildItem -Path C:\Users -Recurse -Include chrome.exe, msedge.exe, opera.exe, brave.exe, vivaldi.exe -ErrorAction SilentlyContinue' via PowerShell remoting or a startup script to enumerate all browser executables including user-profile-installed copies that bypass enterprise patch management. For Linux endpoints, run 'find /home /opt /usr -name chrome -o -name chromium 2>/dev/null'. Force-update Chrome on Windows by running 'C:\Program Files\Google\Chrome\Application\chrome.exe --force-update' or by pushing a registry key to GoogleUpdate. Document any discovered shadow IT browsers as unauthorized software per CIS 2.3 and remove or exception-document them before sign-off.

Evidence: Before eradication, collect the full installed software list from each host (Windows: 'Get-WmiObject Win32_Product' or registry enumeration of HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall) to document which Chromium-based browser versions were present at time of incident — this establishes the exposure inventory for any downstream forensic or regulatory review. Preserve any malicious extension artifacts from Chrome/Edge profile directories ('%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions' and the Edge equivalent) since a successful CVE-2026-11645 exploit chain may have installed a persistence extension post-sandbox-escape; hash and archive these directories before overwriting via update.

Step 4: Recovery — After patching, re-query endpoint management to confirm 100% version compliance. Run a browser process integrity check via EDR to confirm no persistence artifacts remain in browser profile directories or extensions. Monitor web proxy logs for 48 hours post-patch for any continued anomalous outbound connections from browser processes. Validate that browser auto-update policies are enforced and functioning. Reference: NIST AU-6, D3-SFA (System File Analysis).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without EDR for browser profile integrity checking: use PowerShell to enumerate and hash all files in '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\' and compare against a known-good baseline or VirusTotal bulk hash lookup (free API tier). For persistence via malicious extensions specifically, parse the 'manifest.json' in each extension subdirectory for suspicious permissions such as 'nativeMessaging', 'debugger', or broad 'tabs' access that would be consistent with a post-exploit persistence implant. Monitor outbound connections from browser processes for 48 hours using Wireshark captures or Windows Firewall audit logs (Event ID 5156) filtered on chrome.exe and msedge.exe as initiating applications, flagging any connections to IPs or domains not in the organization's baseline.

Evidence: Capture and preserve the full Chrome and Edge extension directories ('%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\' and '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Extensions\') from any host identified as potentially compromised during detection — a V8 exploit post-sandbox-escape commonly persists via a malicious or trojanized browser extension that survives the browser update. Collect Windows Firewall and proxy logs showing post-patch outbound connections initiated by browser processes to identify any C2 beaconing that persisted after the vulnerability was patched, indicating a full compromise occurred rather than a failed exploitation attempt.

Step 5: Post-Incident — Review browser update deferral policies; this zero-day demonstrates that any patch delay window is an active exposure window for browser CVEs. Assess whether your software inventory (CIS 2.1) captures all Chromium-based browsers, not only Chrome and Edge. Evaluate web content filtering and

DNS-based threat blocking to reduce drive-by exposure surface (D3-PBWSAM — Proxy-based Web Server Access Mediation). Consider whether users require all Chromium-based browsers or whether the approved list can be narrowed. Reference: CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 4.6, NIST CM-7 (no mapped control in provided knowledge base for CM-7 — see NIST SP 800-53 Rev. 5 directly).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without commercial web filtering: configure DNS-based blocking using Pi-hole or a free-tier Cloudflare Gateway account with newly-registered-domain (NRD) blocking enabled — this directly reduces the T1189 drive-by delivery attack surface that CVE-2026-11645 relies on. Formalize a browser allowlist policy by Group Policy (Windows) or MDM configuration profile (macOS/iOS) that blocks execution of unapproved Chromium-based browser binaries not managed by enterprise update policy. Document the deferral policy gap identified in this incident and set Chrome and Edge enterprise update policies to 'Update policy override' = 'Always allow updates' in Group Policy (HKLM:\SOFTWARE\Policies\Google\Update\UpdateDefault = 1).

Evidence: Produce a post-incident timeline documenting: (1) the date CVE-2026-11645 was publicly disclosed, (2) the date the patched Chrome/Edge versions were available, (3) the date your organization achieved 100% patch compliance — the delta between these dates is the organization's actual exposure window and is required input for any regulatory breach notification assessment or executive risk reporting. Archive all detection artifacts (Crashpad dumps, proxy logs, Sysmon events, extension directory hashes) per your retention policy under NIST AU-11 (Audit Record Retention) to support any downstream forensic review if a compromised host is later identified.

Detection Guidance

Primary detection signal: browser version compliance gaps. Query your endpoint management platform (Intune, SCCM, Jamf) or EDR for all Chrome and Edge version strings; any installation below the patched release threshold is exposed. In your SIEM, create detections for: (1) renderer process crashes (Windows Event Log: Application crashes with chrome.exe or msedge.exe as the faulting application), (2) unusual child process creation from browser parent processes (EDR process tree: chrome.exe or msedge.exe spawning cmd.exe, powershell.exe, wscript.exe, or other execution hosts), and (3) unexpected outbound network connections from browser child processes to non-CDN, newly registered, or low-reputation domains. Web proxy logs: flag high-frequency visits to newly registered domains or domains with no categorization. No confirmed IOCs have been published at this time. Reference: NIST AU-6 (Audit Record Review), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs).

Framework Mappings

MITRE-ATTACK

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

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** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

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
T1189	Drive-by Compromise	Initial-Access
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Google patches Chrome zero-day exploited in the wild (CVE-2026 ...	https://www.helpnetsecurity.com/2026/06/09/google-chrome-zero-day-c...	T3
CVE-2026-11645, Chrome V8 Zero-Day in Active Exploitation	https://www.penligent.ai/hackinglabs/cve-2026-11645-chrome-v8-zero-...	T3
Google Chrome CVE-2026-11645 : r/PatchMyPC - Reddit	https://www.reddit.com/r/PatchMyPC/comments/1u15hbn/google_chrome_c...	T3
CVE-2026-11645 Common Vulnerabilities and Exposures | SUSE	https://www.suse.com/security/cve/CVE-2026-11645.html	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-11645	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-11645	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-09 19:29 UTC by TJS Security Command Center