Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

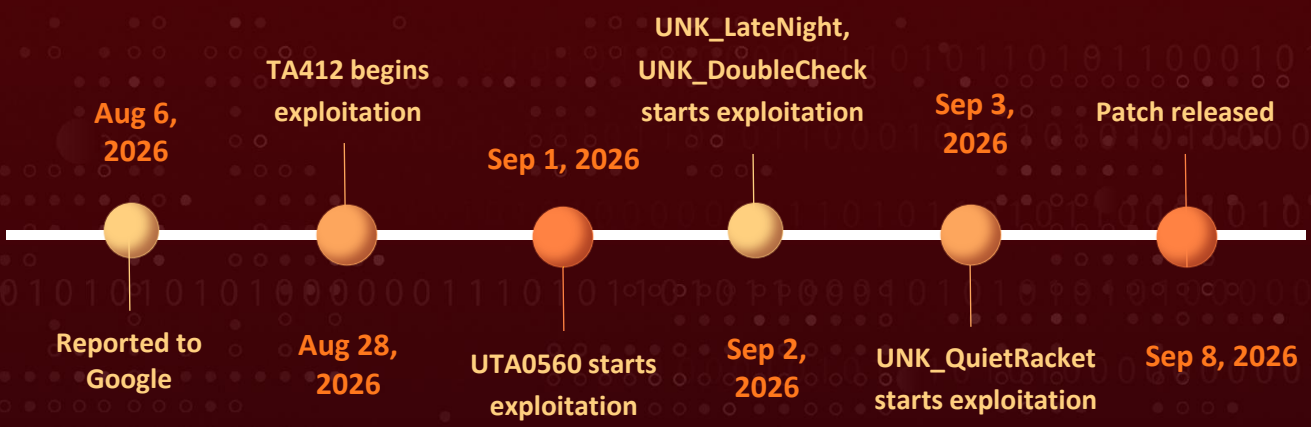
Patch-Gap Panic: Chrome V8 Zero-Day Fuels the BlueMoon Espionage Wave

Date of Publication	Admiralty Code	TA Number
September 11, 2026	A1	TA2026266

Summary

First Seen: August 6, 2026
Affected Product: Google Chrome
Targeted Industries: Non-governmental organizations, aerospace and defense-industrial firms, mining and physical commodity traders, manufacturing entities, and government and financial-sector entities
Targeted Countries: US, Vietnam, Indonesia, Singapore
Threat Actor: TA412 (aka JungleBamboo, APT31, Violet Typhoon, TIDE CASTLE, Judgment Panda, Zirconium, RedBravo, Bronze Vinewood, Red Keres), UTA0560, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket
Malware: GRIMWEDGE, SUPERSTOMP, LONGTALE (aka GemStone), ShadowPad
Impact: Google has patched CVE-2026-87491, an out-of-bounds write flaw in the V8 JavaScript and WebAssembly engine that powers Google Chrome and other Chromium-based browsers. Google has confirmed the flaw is being actively exploited in the wild, making it the seventh Chrome zero-day of 2026 to see real-world use. A successful attacker gains arbitrary code execution inside the Chrome renderer sandbox with nothing more than a click on a crafted link, and the fix reached the Chromium source tree weeks before the stable Chrome release, creating a patch-gap window that exploit developers moved quickly to weaponise. The vulnerability was patched in Chrome 153.0.8010.36 for Linux and 153.0.8010.36/.37 for Windows and macOS on September 8, 2026.

Exploitation Timeline



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-87491	Google Chromium V8 Out of Bounds Write Vulnerability	Google Chrome (V8 Engine)	✓	✓	✓

Vulnerability Details

#1

CVE-2026-87491 is an out-of-bounds write weakness (CWE-787) inside V8, the JavaScript and WebAssembly engine at the heart of Google Chrome and every Chromium-based browser. Google's advisory classifies the flaw with a Medium Chromium security severity. Still, that rating sits alongside a rare and consequential admission from the vendor: an exploit for the bug already exists in the wild, which sharply raises its operational risk.

#2

Technically, the vulnerability lets a specially crafted HTML page trigger a write beyond the boundaries of a V8-managed memory buffer. In a JIT-driven engine that continuously manages compact object layouts, that kind of memory corruption can be steered into adjacent structures and used to influence program execution. In the observed in-the-wild exploit chain, the flaw is abused as a WebAssembly-side defect: after an initial V8 primitive gives the attacker arbitrary read/write inside the V8 sandbox, CVE-2026-87491 is invoked to overwrite compiled WebAssembly function bodies with attacker-controlled shellcode, effectively escaping the V8 sandbox.

#3

The delivery surface is entirely browser-native. A victim only has to open a malicious link, an attacker-controlled or compromised web page, a malvertisement, or a redirect chain. When Chrome parses the crafted content, the vulnerable V8 code path fires, memory is corrupted, and shellcode runs inside the renderer process. All Google Chrome desktop builds earlier than 153.0.8010.36 are affected, with the fix shipping in Chrome 153.0.8010.36/.37 for Windows and macOS and 153.0.8010.36 for Linux. Other Chromium-based browsers inherit the fix once they roll in the upstream V8 change.

#4

In-the-wild exploitation of CVE-2026-87491 is tied to a shared exploit kit tracked as BlueMoon, which chains it with a second V8 flaw (CVE-2026-85046, a type-confusion bug used to obtain arbitrary read/write inside the V8 sandbox) and a Windows kernel local privilege escalation (CVE-2026-85880, abused to escape Chrome's sandboxed renderer) to achieve full host compromise from a single click. BlueMoon was first observed on August 28, 2026, in the hands of the China-aligned threat actor TA412 (aka JungleBamboo, APT31), and rapidly adopted within days by additional espionage-motivated clusters including UTA0560, UNK_LateNight, UNK_DoubleCheck, and UNK_QuietRacket. Across observed campaigns, successful exploitation has been used to deliver a mix of post-exploitation payloads including the GRIMWEDGE JScript backdoor, the SUPERSTOMP loader that installs the LONGTALE (aka GemStone) credential-stealing Chrome extension, the ShadowPad backdoor, and Rust-based loaders, against non-governmental organizations, US aerospace and defense-industrial firms, mining and physical commodity traders, Vietnamese manufacturing entities, and government and financial-sector targets across Indonesia and Singapore.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-87491	Google Chrome versions before 153.0.8010.36 on Windows, macOS, and Linux	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Patch Chrome Immediately Across the Fleet: Update every Chrome installation to at least version 153.0.8010.36 on Linux and 153.0.8010.36/.37 on Windows and macOS, then confirm that each browser has actually been restarted so the vulnerable process is no longer live. Because Chrome's staged rollout can stretch over days, do not rely on auto-update alone; use browser or endpoint management tooling to enforce the fixed version and to audit compliance. Users of Microsoft Edge, Brave, Vivaldi, and other Chromium-based browsers should apply their vendor's next security release as soon as it lands.

Hunt for BlueMoon Exploit-Chain Activity: Retrospectively investigate high-value endpoints that were exposed before the September 8 patch. Look for the BlueMoon telltale process tree (chrome.exe spawning cmd.exe, curl.exe, and a dropped msgbox.exe or ChromeUpdate.exe in %TEMP%), sessionStorage keys named v8ctf_exp_attempt, unexpected renderer crashes, scheduled tasks named "Windows Scheduled System", "EdgeCore_AutoUpdate", "MicrosoftEdgeUpdatesTaskMachine", "Avpcheckup", or "GeForceService", the mutex "Dataupcheckinfo", and any Chromium browser extension masquerading as a Google Gemini companion. Correlate browser telemetry with DNS, proxy, and email logs to catch clicks on the actor infrastructure listed in the IoC section.

Tighten Browser and Endpoint Defences: Enable exploit-protection features in EDR and browser-based memory-integrity controls so that renderer memory corruption raises high-fidelity alerts. Restrict outbound access from browser child processes, block newly registered or low-reputation domains, and monitor for unexpected use of curl.exe or msiexec.exe launched from browser context. Watch for Chrome Secure Preferences tampering, since BlueMoon's post-exploitation loaders bypass Chromium's per-preference encrypted-hash protections to silently side-load malicious extensions.

Reduce the Patch-Gap Exposure Window: Treat public Chromium source-code changes as a leading indicator of upcoming Chrome vulnerabilities and shorten the internal turnaround for high-severity browser updates. Where feasible, adopt browser-management policies that force rapid restart after security releases and prefer channels that receive upstream fixes fastest. Pair this with tighter controls on legacy Windows builds (Windows 10 1809 through 22H2, Server 2019/2022, and Windows 11 21H2) that remain viable targets for the paired kernel LPE.

Strengthen Anti-Phishing and Credential Protections: The BlueMoon chain reaches victims almost exclusively through spear-phishing links, so continue investing in email filtering, URL rewriting, and user awareness for socially engineered themes such as donation requests, university outreach, RFQs, and conference invitations. Because the post-exploitation payloads focus heavily on cookie, session, and credential theft, enforce phishing-resistant multi-factor authentication, rotate suspected exposed credentials, and monitor for anomalous session use of authenticated web applications.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link

Tactic	Technique	Sub-technique
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.003: Windows Command Shell
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1176: Browser Extensions	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1055: Process Injection	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
Credential Access	T1056: Input Capture	T1056.001: Keylogging
	T1539: Steal Web Session Cookie	
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	

Tactic	Technique	Sub-technique
Collection	T1005: Data from Local System	
	T1113: Screen Capture	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d17053557bb90298f7b115432b4820a248fdbe678bca31721529b1f51a82343b, 337b48c1cd6dd6e7b8073327082a60e149517fa084ba17b180e041fffa3b130d, 7a52ff23949edee8faa61ce0def6dbca8b7e5943c54d23376cc190762ea3985c, cd0c21f9b32b7feeda1787fccab622dec60ecdf84c0538c08bde3946856b0fa0, b7b0cd6539464ab39c6526e499f86d611faa21c5af945535ebaf187cec543af1, 5995f42a828606705a7339d58a665c229936e81c4e539cdfa115eb46a2eb53d6, 51462a23ac25e1bd0e49b7cae7f3a71f8d2201e22d45175b587e4740b49863cc, 69c1603f3f9015beb0097d0a3bb0f17400c314e2eae65a7eceacd3b93ea570dc, 3b71d721c39fad92a44ddd764bbb34afeae44a5db886d0a4827a399a5fbd367f, 56eda0ac82e06ee609b034306025e67df161c5877399c305c8eaea136e80c951, 59dc108e22cb856c228bbf8a1ab955fb66f0844a07fe10fa0d9fc3823d2cbbcb, e2a59432ce2b0d83ded936374a11fca3d3defaf4aab90eb37fca58683eae32c0, 5eb5645511b00e4f4d73125654eeb3a3930fcf09c65685dc7f03f725331492e3, 779b3e1a470e589d492b99154ba11622fbaebb19b3de694f660c725411b7096d, ff1b49aaec994f4c11f2c9331e739abb4bc3d6abf66ec50ce99709fba35d782b, 7d6f6dcb17a423bdd7715f8a4e34f2939501a761bc9bf7aa005f805ef1f82288, e950d03c58d49e28e31df8afeefca1f3b3d2cd6b697c40adfee1a4f6fe18f004, 353b5bd2780c1b0c07c1283d83cf16cf1e9ec226c17b2d09d56848893f9d98ee, a4a6a04d85eca8d584d939d2437c85a4f291207d8042f2ec002838e336b72ef5, 295fc584f75e94108c9be945977db33ed80421f5d374eab188587c911dffd915,

TYPE	VALUE
SHA256	bc7d24f5cf8937b334966201bdcce8ca9bab6ec5889d40a399d4094dcad73360, b34802a646fc4a8f07ffa09a5fda8bf7327446b22e3d7bb5163dafa1e2a8bb2b, 8453c42904b7b2fea5671b7bff06b2d937632ae29545fd11bc13095627a2805f, f3c64014221a58f3fde88e562662dbd5a1b3dd2b59c86e9e2bc5cb8f671664e7, 87b6b24c06f99900a8aa579caedee1e402015884c925a98dcfb0fb38dfa2de22, ac6bbc4b1f1c62e308781329183a46e18f454c27e66bffa09f343b53ac622b69, ac6806c89e294f390838cb07c015dabec1c8ada06ce5161a0ad50b8a72828141, 3594ad58fb6217fafe9839e53999a90608c2e9f335fa20aece3d53f8c0802726, 3ec3151d8d1278ed966941ac89ea495ef6a80c70613dd9138cc85fc28c9df432, 6e6378d8d404166da89d982e80bc52e19a3f677201258dec1775f100a027a92d,
Domains	cloud[.]shinewrist[.]net, ocr[.]opusaccel[.]top, msbenefit[.]com, gitprogram[.]com, secboxes[.]com, attcdn[.]com, airproducts[.]ink, precipart[.]ink, epsilonsystems[.]net, rocketlabusa[.]ink, spectrolab[.]fit, checrity[.]com, ms[.]checrity[.]com, aurexdefense[.]online, cyclokinetics[.]online, sncorp[.]fit, tcomlp[.]online, bosch-sensortec[.]site, smxtech[.]xyz, lindes[.]ink,

TYPE	VALUE
Domains	silvustechnologies[.]online, worldview[.]fit, emcore[.]ink, airindia[.]fit, airliquide[.]lol, apollohospitals[.]fit, haloengines[.]net, jetoptera[.]co, joinmacket[.]com, openlumakora[.]com, getaiexo[.]com, elixnovorem[.]com, velodynaity[.]com, brianwilli[.]com, fracons[.]com,
Hostname	recommendation-letter[.]secboxes[.]com, asianstudies[.]secboxes[.]com, materials-project[.]secboxes[.]com, project[.]secboxes[.]com, evidence[.]msbenefit[.]com, data[.]attcdn[.]com, extension-management-portal[.]centerfjdr658[.]workers[.]dev, extension-management-portal[.]kmjukilo-lkjh[.]workers[.]dev, wcce[.]joinmacket[.]com, publish[.]openlumakora[.]com, yhv41nji[.]workers[.]dev, eduac[.]workers[.]dev, daoahueb[.]workers[.]dev, v93xdd5g[.]workers[.]dev, black-flower-9250[.]v93xdd5g[.]workers[.]dev, dns[.]elixnovorem[.]com, dns[.]getaiexo[.]com, dns[.]velodynaity[.]com, mailtbox[.]workers[.]dev, vncdc[.]mailtbox[.]workers[.]dev, homepage[.]brianwilli[.]com, 1a062f4982564d6d19a76884ce8bcbb6[.]r2[.]cloudflarestorage[.]com,
IPv4	206[.]166[.]251[.]164, 79[.]133[.]56[.]90,
URLs	hxxps[:]//cloud[.]shinewrist[.]net/<removed>/Files1[.]html, hxxps[:]//cloud[.]shinewrist[.]net/<removed>/react[.]min[.]js, hxxps[:]//cloud[.]shinewrist[.]net/<removed>/page[.]html, hxxps[:]//photos[.]msbenefit[.]com/fb/w3z, hxxps[:]//photos[.]msbenefit[.]com/fa/t3,

TYPE	VALUE
URLs	hxxps[:]//proof[.]gitprogram[.]com/a4/j8, hxxps[:]//xyz0102[.]gitprogram[.]com/a001, hxxps[:]//project[.]secboxes[.]com/ChromeUpdate[.]exe, hxxps[:]//recommendation-letter[.]secboxes[.]com/ChromeUpdate[.]exe, hxxps[:]//download[.]secboxes[.]com[:]443/dist[.]zip, hxxps[:]//api-prod[.]secboxes[.]com[:]443/download, hxxps[:]//evidence[.]msbenefit[.]com/msgbox[.]exe, hxxps[:]//zki0y83[.]msbenefit[.]com[:]443/feed, hxxps[:]//app[.]eduac[.]workers[.]dev/Service, hxxps[:]//app[.]eduac[.]workers[.]dev/Updateac, hxxps[:]//small-union-7018[.]daoahueb[.]workers[.]dev/, hxxps[:]//snowy-block-ae0a[.]daoahueb[.]workers[.]dev/, hxxps[:]//homepage[.]brianwilli[.]com/d/calibre-launcher[.]dll, hxxps[:]//homepage[.]brianwilli[.]com/d/wint[.]exe, hxxps[:]//homepage[.]brianwilli[.]com/d/85rY[.]dat, hxxps[:]//homepage[.]brianwilli[.]com/d/SysPr[.]prx, hxxps[:]//1a062f4982564d6d19a76884ce8bcbb6[.]r2[.]cloudflarestorage[.]com/datago/krita[.]exe, hxxps[:]//1a062f4982564d6d19a76884ce8bcbb6[.]r2[.]cloudflarestorage[.]com/datago/krita[.]dll, hxxps[:]//1a062f4982564d6d19a76884ce8bcbb6[.]r2[.]cloudflarestorage[.]com/datago/SysPr[.]prx, hxxps[:]//1a062f4982564d6d19a76884ce8bcbb6.r2.cloudflarestorage[.]com
Email	ircribbin77[@]hotmail[.]com, zfg[.]rc[.]420[@]gmail[.]com, laylowthiago[@]gmail[.]com, susan[.]thomas[.]90[@]outlook[.]com, mariedubois1917[@]outlook[.]com, reallifetalktv2[@]gmail[.]com, faizus123[@]outlook[.]com, firda[.]kemkes[@]outlook[.]com, faizus123[@]proton[.]me, dewiinpermata[@]outlook[.]com, radhikadas07[@]outlook[.]com, jeannifer[.]suryajaya[@]outlook[.]com, siti[.]nurhaliza2026[@]outlook[.]com, ditjenpajakri2026[@]outlook[.]com
Mutex	Dataupcheckinfo
Registry Key	HKCU\SOFTWARE\Classes\CLSID\{5D4CFCB7-222C-4CA3-96B6-1F8195FBBB4B}\InprocServer32

Patch Link

https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html

https://www.proofpoint.com/us/blog/threat-insight/once-bluemoon-multiple-state-aligned-threat-actors-rapidly-adopt-novel-exploit

https://www.volexity.com/blog/2026/09/09/mind-the-patch-gap-multiple-chinese-threat-actors-chain-0-day-exploits-in-chrome-windows/

https://www.hivepro.com/threat-advisory/cve-2026-85046-chrome-v8-type-confusion-zero-day-exploited-in-the-wild

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 11, 2026 • 09:00 AM

More at www.hivepro.com