VULNERABILITY STATUS · DCP WORKER FOR WINDOWS · V8 AND WEBGPU (DAWN)

Open V8 vulnerabilities: none known

Installer **dcp-worker-windows-x64.msi 8.0.1, pre-release build 3100729098** Engines **V8 15.8.62.61 · Dawn, Chrome 158 branch**
Status as of **November 22, 2026**

> V8 is the JavaScript and WebAssembly engine that runs job code in the worker's evaluator. Every V8 vulnerability disclosed in Chrome security releases from March 24 to November 18, 2026 is fixed in this build. The engine is at least at the patch level of the current Chrome stable release. The three vulnerabilities disclosed for Chrome 157 and 158 in Dawn, the WebGPU engine used for GPU jobs, are also fixed (page 2).

94	94	0	64 / 21 / 9
V8 CVES IN SCOPE	FIXED	OPEN	HIGH / MEDIUM / LOW

Engine version

The evaluator uses V8 15.8.62.61. Chrome 158.0.8127.36, the stable release of November 17, 2026, ships V8 15.8.62.31. This build contains that exact engine plus the 30 security and stability merges Google added to V8's 15.8 branch through November 20. V8 is embedded through the Node.js development line (28.0.0-pre), because no Node.js release yet carries V8 15.8.

How the status was verified

- **Scope.** Every Chrome stable-channel security release from March 24 to November 18, 2026; every CVE whose component is V8, Turbofan, Maglev or WebAssembly (94 CVEs).
- **Engine lineage.** Chrome 158's V8 (15.8.62.31) is an ancestor of this build's V8 in Google's source history, so every V8 fix Chrome has shipped is included.
- **Fix commits.** For 89 CVEs the fix commit is public; each one was located in this engine's source, either before the 15.8 branch point or as a branch merge. The other 5 have no public fix commit; Google shipped their fixes in Chrome releases up to 158, whose engine this build contains.
- **Regression tests.** V8's published regression tests for these CVEs that can run outside V8's own test shell all pass on this engine on Windows (18 of 18). 11 of them fail on an engine without the fixes, which confirms the tests detect the flaws.

Engine configuration notes

- The engine is built as Node.js builds it: without V8's in-heap memory sandbox (pointer compression off). The evaluator's Windows restrictions apply instead: each slice's process has no network access (Windows Firewall), cannot start programs, runs with no privileges at Medium integrity under Windows' exploit mitigations, and ends when the screensaver is dismissed.
- The engine's debugger is never enabled in production; the evaluator creates it only when started with a debugging port, which the service does not pass.
- Each evaluator process runs one JavaScript context, with no ES-module loading, no cross-origin security tokens and experimental features at their defaults.

WebGPU engine (Dawn)

GPU jobs use Dawn, the WebGPU engine from Chrome, inside the same evaluator. This build's Dawn comes from Chrome 158's branch (chromium/8127) as of November 20, 2026, including that day's fix for oversized strides in `Queue::WriteTexture`. Dawn vulnerabilities disclosed in Chrome 157 and 158 security releases are fixed in the Chrome release whose Dawn this build uses:

CVE	SEVERITY	ISSUE	FIXED IN CHROME	STATUS
CVE-2026-126877	Not rated	Use after free in Dawn	157.0.8103.78	Fixed · in Chrome 158 Dawn
CVE-2026-130977	High	Uninitialized resource in Dawn	158.0.8127.36	Fixed · in Chrome 158 Dawn
CVE-2026-131066	Medium	Uninitialized resource in Dawn	158.0.8127.36	Fixed · in Chrome 158 Dawn

Chromium keeps the details of recent bugs private for some weeks, so whether each one affects the way the worker uses Dawn (outside a browser) cannot always be confirmed; all three are fixed either way. Google had not published a severity for CVE-2026-126877 when this list was made.

Staying current

Google publishes V8 and Dawn fixes with every Chrome security release, currently every one to two weeks. The evaluator's engines follow Chrome's stable branches, and updated worker packages follow those releases. Fixes Google has made but not yet released are not in any public engine, including Chrome's, until Google releases them.

Appendix: V8 CVEs in scope

Disclosed: date of the Chrome release notes that listed the CVE. "Fix verified in engine": the public fix commit is present in this build's V8. "In Chrome 158 engine": no public fix commit; fixed in the Chrome engine this build contains.

CVE	SEVERITY	ISSUE	DISCLOSED	STATUS
CVE-2026-3926	Medium	Out of bounds read in V8	2026-03-24	Fixed · in Chrome 158 engine (no public commit)
CVE-2026-5861	High	Use after free in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-5862	High	Inappropriate implementation in V8	2026-04-22	Fixed · in Chrome 158 engine (no public commit)
CVE-2026-5863	High	Inappropriate implementation in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-5865	High	Type Confusion in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-5871	High	Type Confusion in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-5873	High	Out of bounds read and write in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-6301	High	Type Confusion in Turbofan	2026-04-22	Fixed · fix verified in engine
CVE-2026-6307	High	Type Confusion in Turbofan	2026-04-22	Fixed · fix verified in engine
CVE-2026-5892	Medium	Race in V8	2026-04-22	Fixed · in Chrome 158 engine (no public commit)
CVE-2026-6363	Medium	Type Confusion in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-5904	Low	Use after free in V8	2026-04-22	Fixed · fix verified in engine
CVE-2026-10904	High	Inappropriate implementation in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10910	High	Type Confusion in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10935	High	Inappropriate implementation in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10936	High	Type Confusion in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10963	High	Integer overflow in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10964	High	Integer overflow in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10987	High	Integer overflow in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10989	High	Inappropriate implementation in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11645	High	Out of bounds memory access in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11649	High	Use after free in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11650	High	Use after free in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-10991	Medium	Use after free in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11050	Medium	Use after free in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11075	Medium	Out of bounds read in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11173	Medium	Out of bounds write in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11185	Medium	Use after free in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-11211	Medium	Integer overflow in V8	2026-06-17	Fixed · fix verified in engine
CVE-2026-78899	High	Use after free in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-78938	High	Type confusion in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-79236	High	Type confusion in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-84326	High	Uninitialized resource in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-85045	High	Race condition in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-85046	High	Type confusion in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-78901	Medium	Race condition in V8	2026-09-08	Fixed · fix verified in engine

CVE	SEVERITY	ISSUE	DISCLOSED	STATUS
CVE-2026-78910	Medium	Buffer overflow in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-79097	Medium	Use after free in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-78956	Low	Type confusion in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-79045	Low	Type confusion in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-79197	Low	Use after free in V8	2026-09-08	Fixed · fix verified in engine
CVE-2026-102299	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-102302	High	Buffer overflow in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-102321	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-102323	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-102326	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-102328	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-103625	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-95280	High	Race condition in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-95304	High	Out of bounds write in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-95306	High	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-95342	Low	Missing authorization in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-95380	Low	Type confusion in V8	2026-10-09	Fixed · fix verified in engine
CVE-2026-121057	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121068	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121078	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121079	High	Race condition in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121082	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121094	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121210	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121221	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121226	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121228	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-125344	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126847	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126849	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126864	High	Use after free in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126868	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126874	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126875	High	Missing authorization in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126880	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126889	High	Off-by-one error in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126891	High	Use after free in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126893	High	Out of bounds write in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126896	High	Missing authorization in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126897	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine

CVE	SEVERITY	ISSUE	DISCLOSED	STATUS
CVE-2026-126905	High	Incomplete cleanup in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126908	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126910	High	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-126916	High	Integer overflow in V8	2026-11-18	Fixed · in Chrome 158 engine (no public commit)
CVE-2026-126917	High	Memory corruption in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-131042	High	Use after free in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121048	Medium	Race condition in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121049	Medium	Out of bounds read in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121096	Medium	Incomplete cleanup in V8	2026-11-18	Fixed · in Chrome 158 engine (no public commit)
CVE-2026-121132	Medium	Information leak in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121218	Medium	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-130923	Medium	Out of bounds write in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-130988	Medium	Out of bounds read in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-131087	Medium	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-131097	Medium	Missing authorization in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-121251	Low	Missing authorization in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-130950	Low	Type confusion in V8	2026-11-18	Fixed · fix verified in engine
CVE-2026-131098	Low	Out of bounds read in V8	2026-11-18	Fixed · fix verified in engine

Distributive Corp. Source: Chrome Releases stable-channel posts and V8's public source repository (chromium.googlesource.com/v8/v8) and Dawn's (dawn.googlesource.com/dawn). Questions: contact your Distributive representative.