

webpack — CWE-407 Disclosure Brief

webpack — CWE-407 Disclosure Brief

2026-03-26 · Patch available — awaiting upstream merge

Finding

Three $O(n^2)$ defects in webpack's Hot Module Replacement (HMR) runtime. All patched. Patches ready for upstream review. All three defects are in the HMR runtime bundle — JavaScript code shipped to and executed in the browser on every webpack build with HMR enabled.

The Defects

webpack-0001 (PATCHED — MEDIUM-HIGH): `lib/hmr/JavascriptHotModuleReplacement.runtime.js:74`

```
// Inside getAffectedModuleEffects() - BFS over module dependency graph:
var outdatedModules = [moduleId];
// ...
if (outdatedModules.indexOf(parentId) !== -1) continue; // O(M) per check
outdatedModules.push(parentId);
```

`outdatedModules` is a plain `Array`. `Array.indexOf()` is $O(M)$. Called per module per parent edge during BFS traversal. For M affected modules: **$O(M^2)$ total.**

webpack-0002 (PATCHED — MEDIUM): `JavascriptHotModuleReplacement.runtime.js:101`

```
// addAllToSet helper - called to merge module lists:
function addAllToSet(a, b) {
  for (var i = 0; i < b.length; i++) {
    var item = b[i];
    if (a.indexOf(item) === -1) a.push(item); // O(N) per insertion
  }
}
```

`Array.indexOf()` scans the entire accumulator for every new item. For N items: **$O(N^2)$.**

webpack-0003 (PATCHED — MEDIUM): `lib/hmr/HotModuleReplacement.runtime.js:60,67`

```
// Inside createRequire() - the hot require() wrapper:
if (module.parents.indexOf(parentId) === -1) // O(P)
  module.parents.push(parentId);
// ...
if (me.children.indexOf(request) === -1) // O(C)
  me.children.push(request);
```

Every `require()` call in the HMR hot path deduplicates parents and children arrays using `indexOf`. In a large module graph with many `require()` calls: **$O(P^2 + C^2)$.**

Complexity Proof

webpack-0001 BFS: For M affected modules in the BFS frontier: - Each enqueue step checks

`outdatedModules.indexOf(parentId)`: up to M comparisons - Called M times total - Total: $1 + 2 + \dots + M = O(M^2)$

At $M=200$: defective=19,900 comparisons, fixed=200. **Measured ratio: 100×**

webpack-0002: For N items to add: - Each `indexOf()` scans up to N entries in accumulator - Total: **$O(N^2)$**

webpack-0003: Per `require()` call, $O(P)$ parents scan + $O(C)$ children scan.

Impact

webpack is the most widely deployed JavaScript module bundler. webpack 5 powers millions of web applications. HMR is enabled by default in every webpack dev server — it runs in-browser during development.

`getAffectedModuleEffects()` executes on every file save during hot reload. Large frontend applications (thousands of modules, complex dependency graphs) maximize M and hit the worst case on every hot reload.

`addAllToSet` and the hot `require()` path run on every HMR update cycle. Applications with shared module graphs — monorepos, design systems, large SPA codebases — are most affected.

The Fix

webpack-0001: Shadow `outdatedModules` array with a companion `Set`:

```
// CWE-407 fix: shadow array with Set for O(1) dedup.
var outdatedModules = [];
var outdatedModulesSet = new Set([moduleId]);
outdatedModules.push(moduleId);
// Replace: if (outdatedModules.indexOf(parentId) !== -1) continue;
if (outdatedModulesSet.has(parentId)) continue;
outdatedModulesSet.add(parentId);
outdatedModules.push(parentId);
```

webpack-0002: Maintain a companion `Set` alongside the accumulator array:

```
// CWE-407 fix: companion Set for O(1) dedup in addAllToSet.
function addAllToSet(a, b) {
  if (!a._set) a._set = new Set(a);
  for (var i = 0; i < b.length; i++) {
    if (!a._set.has(b[i])) { a.push(b[i]); a._set.add(b[i]); }
  }
}
```

webpack-0003: Use `Set` companions for parents and children:

```
// CWE-407 fix: Set companions for parents/children in hot require path.
if (!module._parentsSet) module._parentsSet = new Set(module._parents);
if (!module._parentsSet.has(parentId)) {
  module._parents.push(parentId);
  module._parentsSet.add(parentId);
}
```

Patch

Fix available: - `defects/webpack/patch/webpack-0001-hmr-outdated-set.patch` - `defects/webpack/patch/webpack-0002-hmr-parents-children-set.patch`

Unit test: 4/4 pass. webpack-0001 at M=200: defective=19,900, fixed=200, **100× speedup**. webpack-0002 at N=200: same ratio.

What We Ask

A patch is ready for review.

1. Confirm receipt and assign a GitHub Security Advisory (webpack/webpack).
2. Assess severity — webpack-0001 fires on every hot reload in webpack dev server.
3. Coordinate a disclosure date — we are targeting 90 days from first contact.
4. We will credit the webpack team in the public disclosure. Preferred acknowledgment format welcome.

Contact: see cover email. This brief is confidential until coordinated disclosure.