Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in underscore.deep

High mcab published GHSA-8j79-hfj5-f2xm on Jun 27

Package

underscore.deep (npm)

Affected versions

<0.5.2

Patched versions

0.5.3

Description

Impact

What kind of vulnerability is it? Who is impacted?

`underscore.deep` is vulnerable to prototype pollution.

An attacker can craft a malicious payload and pass it to `deepFromFlat`, which would pollute any future Objects created.

Any users that have `deepFromFlat` or `deepPick` (due to its dependency on `deepFromFlat`) in their code should upgrade.

Patches

Has the problem been patched? What versions should users upgrade to?

This is patched in 0.5.3. Users should upgrade to 0.5.3.

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

Modifying `deepFromFlat` to prevent specific keywords will prevent this from happening.

For more information

If you have any questions or comments about this advisory, feel free to open an issue in Clever/underscore.deep. This was triaged in https://huntr.dev/bounties/23204932-72b2-419d-b5f0-34a130752d82/.

Severity

High

CVE ID

CVE-2022-31106

Weaknesses

CWE-1321

Credits

 Sampaguitas