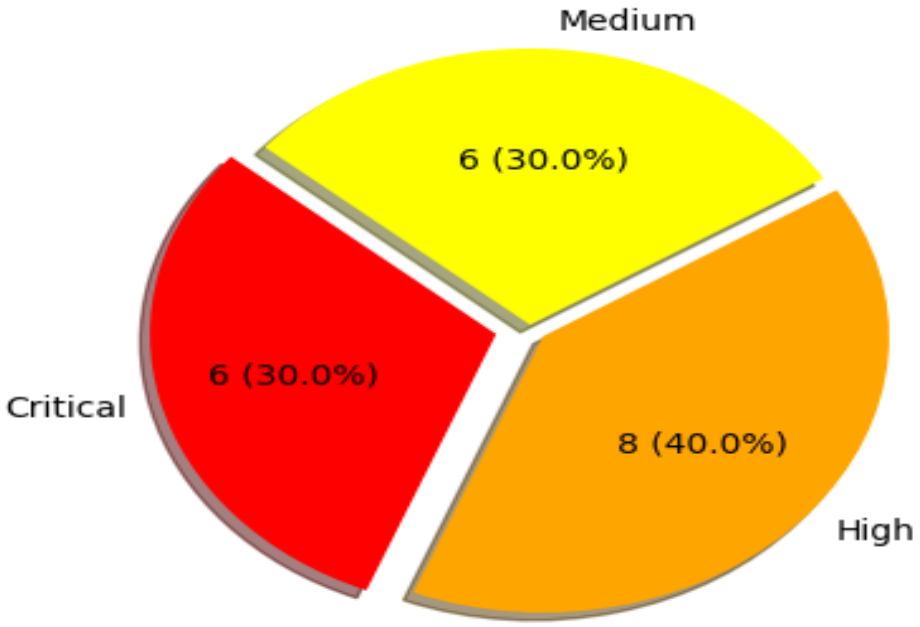
ios-triage: Vulnerabilities Scan Report

Vulnerability severity counts:



Package vulnerability information:

NAME	INSTALLED	FIXED-IN	TYPE	VULNERABILITY	SEVERITY	EPSS%	RISK
handlebars	4.2.0	4.3.0	npm	GHSA-w457-6q6x-cgp9	Critical	94.62	15.9
handlebars	4.2.0	4.7.7	npm	GHSA-765h-qjxv-5f44	Critical	89.53	5.0
handlebars	4.2.0	4.7.7	npm	GHSA-f2jv-r9rf-7988	Critical	88.38	4.1
plist	3.0.1	3.0.5	npm	GHSA-4cpg-3vgw-4877	Critical	83.92	2.1
minimist	0.0.10	0.2.4	npm	GHSA-xvch-5gv4-984h	Critical	77.34	1.1
xmldom	0.1.27		npm	GHSA-crh6-fp67-6883	Critical	76.64	1.0
lodash	4.17.15	4.17.19	npm	GHSA-p6mc-m468-83gw	High	86.61	2.4
async	2.6.1	2.6.4	npm	GHSA-fwr7-v2mv-hh25	High	74.71	0.7
lodash	4.17.15	4.17.21	npm	GHSA-35jh-r3h4-6jhm	High	73.98	0.6
handlebars	4.2.0	4.5.3	npm	GHSA-3cqr-58rm-57f8	High	65.94	0.4
handlebars	4.2.0	4.4.5	npm	GHSA-62gr-4qp9-h98f	High	48.16	0.2
handlebars	4.2.0	4.5.2	npm	GHSA-2cf5-4w76-r9qv	High	N/A	N/A
handlebars	4.2.0	4.5.3	npm	GHSA-g9r4-xpmj-mj65	High	N/A	N/A
handlebars	4.2.0	4.5.3	npm	GHSA-q2c6-c6pm-g3gh	High	N/A	N/A
xmldom	0.1.27	0.5.0	npm	GHSA-h6q6-9hqw-rwfv	Medium	67.67	0.3
xmldom	0.1.27		npm	GHSA-5fg8-2547-mr8q	Medium	59.32	0.2
lodash	4.17.15	4.17.21	npm	GHSA-29mw-wpgm-hmr9	Medium	50.59	0.1
minimist	0.0.10	0.2.1	npm	GHSA-vh95-rmgr-6w4m	Medium	48.47	0.1

color-string	1.5.3	1.5.5	npm	GHSA-257v-vj4p-3w2h	Medium	44.10	0.1
handlebars	4.2.0	4.4.5	npm	GHSA-f52g-6jhx-586p	Medium	N/A	N/A

Vulnerability patch recommendations:

Vulnerabilities without available patches:

Consider removing or replacing **xmldom** (severity: **Critical**) as no patched version is currently available.

Critical patch recommendations:

Update **handlebars** to version **4.7.7** or later.
Update **plist** to version **3.0.5** or later.
Update **minimist** to version **0.2.4** or later.

High patch recommendations:

Update **lodash** to version **4.17.21** or later.
Update **async** to version **2.6.4** or later.

Medium patch recommendations:

Update **xmldom** to version **0.5.0** or later.
Update **color-string** to version **1.5.5** or later.

Detailed vulnerability information:

GHSA-w457-6q6x-cgp9

Id	GHSA-w457-6q6x-cgp9
Details	Versions of `handlebars` prior to 3.0.8 or 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Objects' `__proto__` and `__defineGetter__` properties, which may allow an attacker to execute arbitrary code through crafted payloads. ## Recommendation Upgrade to version 3.0.8, 4.3.0 or later.
CWEs	CWE-1321, CWE-74
Published	2019-12-26T17:58:13Z

GHSA-765h-qjxv-5f44

Id	GHSA-765h-qjxv-5f44
Details	The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling options to compile templates coming from an untrusted source.
CWEs	CWE-1321
Published	2022-02-10T23:51:42Z

GHSA-f2jv-r9rf-7988

Id	GHSA-f2jv-r9rf-7988
Details	The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source.
CWEs	CWE-94
Published	2021-05-06T15:57:44Z

GHSA-p6mc-m468-83gw

Id	GHSA-p6mc-m468-83gw
Details	Versions of lodash prior to 4.17.19 are vulnerable to Prototype Pollution. The functions `pick`, `set`, `setWith`, `update`, `updateWith`, and `zipObjectDeep` allow a malicious user to modify the prototype of Object if the property identifiers are user-supplied. Being affected by this issue requires manipulating objects based on user-provided property values or arrays. This vulnerability causes the addition or modification of an existing property that will exist on all objects and may lead to Denial of Service or Code Execution under specific circumstances.
CWEs	CWE-1321, CWE-770
Published	2020-07-15T19:15:48Z

GHSA-4cpg-3vgw-4877

Id	GHSA-4cpg-3vgw-4877
Details	Prototype pollution vulnerability via `.parse()` in Plist allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.
CWEs	CWE-1321
Published	2022-02-18T00:00:33Z

GHSA-xvch-5gv4-984h

Id	GHSA-xvch-5gv4-984h
Details	Minimist prior to 1.2.6 and 0.2.4 is vulnerable to Prototype Pollution via file `index.js`, function `setKey()` (lines 69-95).
CWEs	CWE-1321
Published	2022-03-18T00:01:09Z

GHSA-crh6-fp67-6883

Id	GHSA-crh6-fp67-6883
Details	### Impact xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to https://nvd.nist.gov/vuln/detail/CVE-2022-39299 and is a potential issue for dependents. ### Patches Update to `@xmldom/xmldom@~0.7.7`, `@xmldom/xmldom@~0.8.4` (dist-tag `latest`) or `@xmldom/xmldom@>=0.9.0-beta.4` (dist-tag `next`). ### Workarounds One of the following approaches might help, depending on your use case: - Instead of searching for elements in the whole DOM, only search in the `documentElement`. - Reject a document with a document that has more then 1 `childNode`. ### References - https://nvd.nist.gov/vuln/detail/CVE-2022-39299 - https://github.com/jindw/xmldom/issues/150 ### For more information If you have any questions or comments about this advisory: * Email us at security@xmldom.org
CWEs	CWE-1288, CWE-20
Published	2022-11-01T17:29:11Z

GHSA-fwr7-v2mv-hh25

Id	GHSA-fwr7-v2mv-hh25
Details	A vulnerability exists in Async through 3.2.1 for 3.x and through 2.6.3 for 2.x (fixed in 3.2.2 and 2.6.4), which could let a malicious user obtain privileges via the `mapValues()` method.
CWEs	CWE-1321
Published	2022-04-07T00:00:17Z

GHSA-35jh-r3h4-6jhm

Id	GHSA-35jh-r3h4-6jhm
Details	`lodash` versions prior to 4.17.21 are vulnerable to Command Injection via the template function.
CWEs	CWE-77, CWE-94
Published	2021-05-06T16:05:51Z

GHSA-3cqr-58rm-57f8

Id	GHSA-3cqr-58rm-57f8
Details	Handlebars before 3.0.8 and 4.x before 4.5.3 is vulnerable to Arbitrary Code Execution. The lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript. This can be used to run arbitrary code on a server processing Handlebars templates or in a victim's browser (effectively serving as XSS).
CWEs	CWE-94
Published	2022-02-10T20:38:19Z

GHSA-h6q6-9hqw-rwfv

Id	GHSA-h6q6-9hqw-rwfv
Details	### Impact xmldom versions 0.4.0 and older do not correctly preserve [system identifiers](https://www.w3.org/TR/2008/REC-xml-20081126/#d0e4313), [FPIs](https://en.wikipedia.org/wiki/Formal_Public_Identifier) or [namespaces](https://www.w3.org/TR/xml-names11/) when repeatedly parsing and serializing maliciously crafted documents. This may lead to unexpected syntactic changes during XML processing in some downstream applications. ### Patches Update to 0.5.0 (once it is released) ### Workarounds Downstream applications can validate the input and reject the maliciously crafted documents. ### References Similar to this one reported on the Go standard library: - https://mattermost.com/blog/coordinated-disclosure-go-xml-vulnerabilities/ ### For more information If you have any questions or comments about this advisory: * Open an issue in [`xmldom/xmldom`](https://github.com/xmldom/xmldom) * Email us: send an email to **all** addresses that are shown by `npm owner ls xmldom`
CWEs	CWE-115, CWE-436
Published	2021-03-12T22:39:39Z

GHSA-5fg8-2547-mr8q

Id	GHSA-5fg8-2547-mr8q
Details	### Impact xmldom versions 0.6.0 and older do not correctly escape special characters when serializing elements removed from their ancestor. This may lead to unexpected syntactic changes during XML processing in some downstream applications. ### Patches Update to one of the fixed versions of `@xmldom/xmldom` (`>=0.7.0`) See issue #271 for the status of publishing `xmldom` to npm or join #270 for Q&A;/discussion until it's resolved. ### Workarounds Downstream applications can validate the input and reject the maliciously crafted documents. ### References Similar to this one reported on the Go standard library: - https://mattermost.com/blog/coordinated-disclosure-go-xml-vulnerabilities/ - https://mattermost.com/blog/securing-xml-implementations-across-the-web/ ### For more information If you have any questions or comments about this advisory: * Open an issue in [`xmldom/xmldom`](https://github.com/xmldom/xmldom) * Email us: send an email to **all** addresses that are shown by `npm owner ls @xmldom/xmldom`
CWEs	CWE-116
Published	2021-08-03T16:57:05Z

GHSA-62gr-4qp9-h98f

Id	GHSA-62gr-4qp9-h98f
Details	Handlebars before 4.4.5 allows Regular Expression Denial of Service (ReDoS) because of eager matching. The parser may be forced into an endless loop while processing crafted templates. This may allow attackers to exhaust system resources.
CWEs	CWE-400
Published	2022-02-10T20:38:22Z

GHSA-29mw-wpgm-hmr9

Id	GHSA-29mw-wpgm-hmr9
Details	All versions of package lodash prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the `toNumber`, `trim` and `trimEnd` functions. Steps to reproduce (provided by reporter Liyuan Chen): ```js var lo = require('lodash'); function build_blank(n) { var ret = "1" for (var i = 0; i < n; i++) { ret += " " } return ret + "1"; } var s = build_blank(50000) var time0 = Date.now(); lo.trim(s) var time_cost0 = Date.now() - time0; console.log("time_cost0: " + time_cost0); var time1 = Date.now(); lo.toNumber(s) var time_cost1 = Date.now() - time1; console.log("time_cost1: " + time_cost1); var time2 = Date.now(); lo.trimEnd(s); var time_cost2 = Date.now() - time2; console.log("time_cost2: " + time_cost2); ```
CWEs	CWE-1333, CWE-400
Published	2022-01-06T20:30:46Z

GHSA-vh95-rmgr-6w4m

Id	GHSA-vh95-rmgr-6w4m
Details	Affected versions of `minimist` are vulnerable to prototype pollution. Arguments are not properly sanitized, allowing an attacker to modify the prototype of `Object`, causing the addition or modification of an existing property that will exist on all objects. Parsing the argument `--__proto__.y=Polluted` adds a `y` property with value `Polluted` to all objects. The argument `--__proto__=Polluted` raises and uncaught error and crashes the application. This is exploitable if attackers have control over the arguments being passed to `minimist`. ## Recommendation Upgrade to versions 0.2.1, 1.2.3 or later.
CWEs	CWE-1321
Published	2020-04-03T21:48:32Z

GHSA-257v-vj4p-3w2h

Id	GHSA-257v-vj4p-3w2h
Details	In the npm package `color-string`, there is a ReDos (Regular Expression Denial of Service) vulnerability regarding an exponential time complexity for linearly increasing input lengths for `hwb()` color strings. Strings reaching more than 5000 characters would see several milliseconds of processing time; strings reaching more than 50,000 characters began seeing 1500ms (1.5s) of processing time. The cause was due to a the regular expression that parses hwb() strings - specifically, the hue value - where the integer portion of the hue value used a 0-or-more quantifier shortly thereafter followed by a 1-or-more quantifier. This caused excessive backtracking and a cartesian scan, resulting in exponential time complexity given a linear increase in input length.
CWEs	CWE-770
Published	2021-06-22T01:14:09Z

GHSA-2cf5-4w76-r9qv

Id	GHSA-2cf5-4w76-r9qv

Details	Versions of `handlebars` prior to 3.0.8 or 4.5.2 are vulnerable to Arbitrary Code Execution. The package's lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript in the system. It can be used to run arbitrary code in a server processing Handlebars templates or on a victim's browser (effectively serving as Cross-Site Scripting). The following template can be used to demonstrate the vulnerability: ```{{#with "constructor"}} {{#with split as |a|}} {{pop (push "alert('Vulnerable Handlebars JS');")}} {{#with (concat (lookup join (slice 0 1)))}} {{#each (slice 2 3)}} {{#with (apply 0 a)}} {{.}} {{/with}} {{/each}} {{/with}} {{/with}} {{/with}}``` ## Recommendation Upgrade to version 3.0.8, 4.5.2 or later.
CWEs	CWE-94
Published	2020-09-04T14:57:38Z

GHSA-g9r4-xpmj-mj65

Id	GHSA-g9r4-xpmj-mj65
Details	Versions of `handlebars` prior to 3.0.8 or 4.5.3 are vulnerable to prototype pollution. It is possible to add or modify properties to the Object prototype through a malicious template. This may allow attackers to crash the application or execute Arbitrary Code in specific conditions. ## Recommendation Upgrade to version 3.0.8, 4.5.3 or later.
CWEs	CWE-1321
Published	2020-09-04T15:06:32Z

GHSA-q2c6-c6pm-g3gh

Id	GHSA-q2c6-c6pm-g3gh
Details	Versions of `handlebars` prior to 3.0.8 or 4.5.3 are vulnerable to Arbitrary Code Execution. The package's lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript in the system. It is due to an incomplete fix for a [previous issue](https://www.npmjs.com/advisories/1316). This vulnerability can be used to run arbitrary code in a server processing Handlebars templates or on a victim's browser (effectively serving as Cross-Site Scripting). ## Recommendation Upgrade to version 3.0.8, 4.5.3 or later.
CWEs	
Published	2020-09-04T15:07:38Z

GHSA-f52g-6jhx-586p

Id	GHSA-f52g-6jhx-586p
Details	Affected versions of `handlebars` are vulnerable to Denial of Service. The package's parser may be forced into an endless loop while processing specially-crafted templates. This may allow attackers to exhaust system resources leading to Denial of Service. ## Recommendation Upgrade to version 4.4.5 or later.
CWEs	CWE-400
Published	2020-09-03T23:20:12Z