KlintonICT
baak-packagejson-test
From: sinopia/package.json

1 CRITICAL
7 HIGH
1 MODERATE
3 LOW

Summary

Total vulnerabilities: 12

Dependency	Type	Updating	Severity
minimatch	Direct	< 3.0.2 → 3.0.2	high
handlebars	Direct	< 3.0.8 → 3.0.8	high
handlebars	Direct	< 3.0.8 → 3.0.8	high
handlebars	Direct	< 3.0.8 → 3.0.8	high
handlebars	Direct	< 4.3.0 → 4.3.0	high
handlebars	Direct	< 3.0.7 → 3.0.7	critical
handlebars	Direct	< 4.0.0 → 4.0.0	high
handlebars	Direct	< 4.0.0 → 4.0.0	moderate
highlight.js	Direct	< 9.18.2 → 9.18.2	low
uglify-js	Indirect	< 2.4.24 → 2.4.24	high
uglify-js	Indirect	< 2.4.24 → 2.4.24	low
uglify-js	Indirect	< 2.6.0 → 2.6.0	low

Total of vulnerable direct dependency: 9

Total of vulnerable indirect dependency: 3

Vulnerabilities

Sort By

Potentially Vulnerable: **minimatch**

Severity: high

Current Usage Version: >=0.2.14 <2.0.0-0

Vulnerable Version: < 3.0.2

Patch Version: 3.0.2

Vulnerability Chaining:

Vulnerabilities and Advisory link: GHSA-hxm2-r34f-qmc5
CVE-2016-10540

Dependency to be updated: minimatch

Update **minimatch** to latest version: >=0.2.14 <2.0.0-0 → 3.0.4

Potentially Vulnerable: **handlebars**

Severity: high

Current Usage Version: 2.x

Vulnerable Version: < 3.0.8

Patch Version: 3.0.8

Vulnerability Chaining:

Vulnerabilities and Advisory link: GHSA-q2c6-c6pm-g3gh

Dependency to be updated: handlebars

Update **handlebars** to latest version: 2.x → 4.7.7

Potentially Vulnerable: **handlebars**

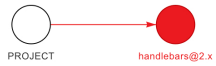
Severity: high

Current Usage Version: 2.x

Vulnerable Version: < 3.0.8

Patch Version: 3.0.8

Vulnerability Chaining:



Vulnerabilities and Advisory link: GHSA-g9r4-xpmj-mj65

Dependency to be updated: handlebars

Update **handlebars** to latest version: 2.x → 4.7.7

Potentially Vulnerable: handlebars

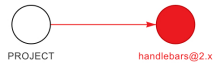
Severity: high

Current Usage Version: 2.x

Vulnerable Version: < 3.0.8

Patch Version: 3.0.8

Vulnerability Chaining:



Vulnerabilities and Advisory link: GHSA-2cf5-4w76-r9qv

Dependency to be updated: handlebars

Update **handlebars** to latest version: 2.x → 4.7.7

Potentially Vulnerable: handlebars

Severity: high

Current Usage Version: 2.x

Vulnerable Version: < 4.3.0

Patch Version: 4.3.0

Vulnerability Chaining:

Vulnerabilities and Advisory link: GHSA-w457-6q6x-cgp9
CVE-2019-19919

Dependency to be updated: handlebars

Update **handlebars** to latest version: 2.x → 4.7.7

Potentially Vulnerable: handlebars

Severity: critical

Current Usage Version: 2.x

Vulnerable Version: < 3.0.7

Patch Version: 3.0.7

Vulnerability Chaining:

Vulnerabilities and Advisory link: GHSA-q42p-pg8m-cqh6

Dependency to be updated: handlebars

Update **handlebars** to latest version: 2.x → 4.7.7

Potentially Vulnerable: handlebars

Severity: high

Current Usage Version: 2.x

Vulnerable Version: < 4.0.0

Patch Version: 4.0.0

Vulnerability Chaining:

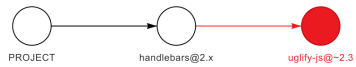
Vulnerabilities and Advisory link:	GHSA-9prh-257w-9277 CVE-2015-8861
Dependency to be updated:	handlebars
Update **handlebars** to latest version:	2.x → 4.7.7

Potentially Vulnerable:	handlebars
Severity:	moderate
Current Usage Version:	2.x
Vulnerable Version:	< 4.0.0
Patch Version:	4.0.0
Vulnerability Chaining:	

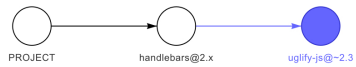
Vulnerabilities and Advisory link:	GHSA-fmr4-7g9q-7hc7 CVE-2015-8861
Dependency to be updated:	handlebars
Update **handlebars** to latest version:	2.x → 4.7.7

Potentially Vulnerable:	highlight.js
Severity:	low
Current Usage Version:	8.x
Vulnerable Version:	< 9.18.2
Patch Version:	9.18.2
Vulnerability Chaining:	

Vulnerabilities and Advisory link:	GHSA-vfrc-7r7c-w9mx CVE-2020-26237
CWEs:	CWE-471: Modification of Assumed-Immutable Data (MAID)
Dependency to be updated:	highlight.js
Update **highlight.js** to latest version:	8.x → 10.7.2

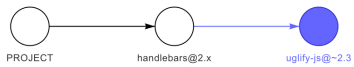
Potentially Vulnerable:	uglify-js
Severity:	high
Current Usage Version:	~2.3
Vulnerable Version:	< 2.4.24
Patch Version:	2.4.24
Vulnerability Chaining:	

Vulnerabilities and Advisory link:	GHSA-g6f4-j6c2-w3p3 CVE-2015-8857
Dependency to be updated:	handlebars
Update **handlebars** to latest version:	2.x → 4.7.7

Potentially Vulnerable:	uglify-js
Severity:	low
Current Usage Version:	~2.3
Vulnerable Version:	< 2.4.24
Patch Version:	2.4.24
Vulnerability Chaining:	

Vulnerabilities and Advisory link:	GHSA-24x7-g49f-h37c

Vulnerabilities and Advisory link:	GHSA-34f7-q49f-h37c CVE-2015-8857
Dependency to be updated:	handlebars
Update **handlebars** to latest version:	2.x → 4.7.7

Potentially Vulnerable:	**uglify-js**
Severity:	low
Current Usage Version:	~2.3
Vulnerable Version:	< 2.6.0
Patch Version:	2.6.0
Vulnerability Chaining:	
Vulnerabilities and Advisory link:	GHSA-c9f4-xj24-8jqx CVE-2015-8858
Dependency to be updated:	handlebars
Update **handlebars** to latest version:	2.x → 4.7.7

Download Report