



# CVE-2018-11537

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-11537
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-19 19:29:00 UTC
<b>Updated</b>	2018-08-23 14:17:00 UTC
<b>Description</b>	Auth0 angular-jwt before 0.1.10 treats whiteListedDomains entries as regular expressions, which allows remote attackers w

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Auth0</a>	<a href="#">Angular-jwt</a>	All	All	All	All
Application	<a href="#">Auth0</a>	<a href="#">Angular-jwt</a>	All	All	All	All

## References

Reference	Source	Link	Tags
CVE-2018-11537: Security Update for angular-jwt Allow List Bypass	CONFIRM	<a href="#">auth0.com</a>	Patch, Vendor Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[995644](#) NodeJs (Npm) Security Update for angular-jwt (GHSA-vm2p-f5j4-mj6g)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**